Universidad
Carlos III de Madrid

TESIS DOCTORAL

Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau

Autor:

Fernandinho Domingos Sanca

Directora:

Dra. D. ª Teresa Rodríguez de las Heras Ballell

DEPARTAMENTO DE DERECHO PRIVADO

Getafe, 25 de enero de 2013

TESIS DOCTORAL

Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau

Autor:

Fernandinho Domingos Sanca

Directora: Dra. D. ª Teresa Rodríguez de las Heras Ballell

Firma del Tribunal Calificador:

Firma

Presidente: (Nombre y apellidos)

Vocal: (Nombre y apellidos)

Secretario: (Nombre y apellidos)

Calificación:

Getafe, de de 2013

EXERGO

La Ley es con relación al alma y a la vida, como la armonía es con relación al oído y a la voz, pues la Ley instruye el alma y con ello regula la vida, como la armonía, educando el oído regula la voz.

Pitágoras de Samos.

ÍNDICE

DEDICATORIA 17
AGRADECIMIENTOS 19
ABREVIATURAS 21
RESUMEN 27
INTRODUCCIÓN 31

CAPITULO PRIMERO

EL COMERCIO ELECTRÓNICO Y LOS MEDIOS DE PAGO ELECTRÓNICOS: ANALISIS DEL PAGO CON TARJETA EN EL COMERCIO ELECTRÓNICO

I. PRECISIONES INTRODUCTORIAS 45
1.1. Comercio electrónico: concepto y modalidades 47
1.1.1. Concepto de comercio electrónico 47
1.1.2. Modalidades de comercio electrónico 50
1.1.2.1. Por cómo se realiza el contrato 50
A. Comercio electrónico directo 50
B. Comercio electrónico indirecto 51
C. Distinción entre el comercio electrónico directo y el comercio electrónico indirecto 53
1.1.2.2. Según los entes intervinientes 53
A. El comercio electrónico entre empresas B2B (Business to Business) 54
B. El comercio electrónico empresa-consumidor (business to consumer B2C) 55
C. El comercio electrónico entre empresa-administración pública B2A 58
D. El comercio electrónico entre consumidor-gobierno C2A 58
E. Comercio electrónico entre consumidores C2C 60
1.2. Concepto de pago electrónico 62
1.3. Concepto de medios de pago electrónicos 65
1.4. Las modalidades de medios de pago en el comercio electrónico 68

A.Los medios de pago tradicionales. 69
B.Los medios de pago electrónicos. 69
1.4.1. Tarjeta bancaria (crédito o débito) 69
1.4.2. Contra-reembolso 70
1.4.3. Transferencia electrónica de fondos 71
1.4.4. Cheque electrónico 72
1.4.5. Monedero electrónico 73
1.4.6. Dinero electrónico 75
1.4.6.1. Análisis de los sistemas de dinero electrónico 80
A.Sistemas basados en un software (software-based) 80
a) Los pioneros en el mercado 80
a1) E-cash 81
a 2) Millicent 81
b) Los nuevos modelos de dinero electrónico 83
b1) Ukash 83
b2) Hal-Cash 84
b 3) Paypal 85
b 4) Skrill (Moneybookers) 85
B. Sistemas basados en hardware 86
a) Cybercash 86
b) Mondex 88
1.5. Tarjeta electrónica de pago y su clasificación 90
1.5.1. Concepto de tarjeta electrónica de pago 94
1.5.2. Clasificación de las tarjetas electrónicas 97
1.5.2.1. Por los elementos personales que intervienen 97
A. Tarjetas bilaterales 98
B- Tarjetas trilaterales 98
1.5.2.2. Por el emisor 99
A.Tarjetas no bancarias (tarjetas de compra) 99
B. Tarjetas bancarias 100
C. Tarjetas financieras 100
1.5.2.3. Por el sistema de liquidación utilizado 100
A. La tarjeta de crédito 100

B. Las tarjetas de débito 102
1.5.3. La diferencia entre las tarjetas de crédito y las de débito 103
1.5.4. Tarjetas de prepago 104
1.5.5. Tarjeta de cargo diferido o tarjeta de compra 106
1.6. Sujetos que intervienen en el uso de tarjeta electrónica 107
1.6.1. La entidad emisora y/o gestora de la tarjeta 108
1.6.2. Titular y/o contratante/solicitante 110
1.6.3. Proveedor de bienes o servicios adherido al sistema de pago con tarjetas 111
1.6.4. Entidad adquirente 112
1.6.5. Entidad franquiciadora 113
1.7. Intermediarios 113
1.7.1. Proveedores de acceso 116
1.7.2. Proveedor de servicios de certificación 116
1.8. Las operativas de pago mediante tarjeta de crédito 120
1.9. Marco jurídico de los medios de pago electrónico 121
1.9.1. Análisis de la Ley 16/2009, de 13 de noviembre, de servicios de pago (LSP) 123
1.9.2. Ámbito de aplicación de la LSP 123
1.9.3. Objeto de la LSP 124
1.9.4. Derechos y obligaciones del proveedor y del usuario de servicio de pago 125
1.10. Ventajas en la utilización de tarjeta como medio pago en el comercio electrónico a través de Internet 128
1.11. Riesgos en la operativa de pago mediante tarjeta de crédito en el comercio electrónico 129
1.12. Tipos de fraudes en medios de pago electrónicos 131
1.12.1. Phishing 132
1.12.2. Pharming 134
1.12.3. Código malicioso 135
1.13. Consideraciones finales 137

CAPÍTULO SEGUNDO

SEGURIDAD EN LOS PAGOS MEDIANTE TARJETA DE CRÉDITO O DÉBITO EN EL COMERCIO ELECTRÓNICO

2. INTRODUCCIÓN 141
2.1. La seguridad en la operativa de pago mediante tarjeta de crédito o débito en el comercio electrónico 142
2.2. Componentes de seguridad exigidos en las transacciones electrónicas . 146
a) Autenticación 147
b) Confidencialidad 147
c) Integridad 149
d) El no rechazo o no repudio 149
2.3. El uso de los métodos criptográficos en las transacciones electrónicas 151
2.3.1. Criptografía: concepto y finalidad 152
2.3.2. Clases de criptografía 154
2.3.2.1. Sistema simétrico o de clave privada 154
2.3.2.2. Sistema asimétrico o de clave pública 156
2.4. La firma digital y la función hash 160
2.4.1. Generación y verificación de la firma digital 163
A. Generación de firma digital 163
B. Verificación de la firma digital 164
2.5. Protocolos de seguridad para la realización de pago mediante el uso del número de las tarjetas a través de Internet 167
2.5.1. Aspecto general 167
2.5.2. Protocolo SSL (Secure Sockets Layer) 168
2.5.2.1. Funcionamiento de SSL 170
2.5.2.2. Sujetos intervinientes en la transacción por medio de SSL 171
2.5.2.3. Ventajas e Inconvenientes del sistema SSL 172
2.5.2.4. Servidores seguros 173
2.5.3. Protocolo SET (Secure Electronic Transaction) 174
2.5.3.1. Servidores seguros 176

2.5.3.2. Entes intervinientes en una operativa de pago con tarjeta de crédito en la que se hace uso del SET 176
2.5.3.3. El procedimiento de pago electrónico con SET..... 179
2.5.3.4. Ventajas e Inconvenientes del SET 182
2.6. Diferencias existente entre el SET y SSL 183
2.7. El protocolo 3DSecure 185
2.8. Proceso de compra con tarjeta visa mediante 3D Secure 187
2.9. La seguridad jurídica en la operativa de pago mediante tarjeta de crédito o débito en el comercio electrónico..... 188
2.10. Consideraciones finales 190

CAPÍTULO TERCERO
RELACIONES JURIDICAS PARA EL PAGO ELECTRÓNICA CON TARJETA
3. PRECISIONES INTRODUCTORIAS..... 197
3.1. El contrato de emisión de la tarjeta..... 199
3.1.1. Concepto..... 199
3.1.2. Caracteres jurídicos del contrato 200
3.2. Tipos de contratos relacionados con el contrato de emisión de tarjeta..... 206
3.2.1. Contrato de apertura de crédito mediante tarjeta..... 206
3.2.1.1. Caracteres..... 210
3.2.2. Contrato de mandato..... 212
3.2.3. Contrato de cuenta corriente bancaria..... 212
3.2.3.1. Concepto..... 213
3.2.3.2. Las diferencias existentes entre el contrato de cuenta corriente bancaria y el contrato de cuenta corriente mercantil..... 215
3.3. Contrato de pasarela de pagos o Terminal de Punto de Venta Virtual.. 217
3.3.1. Concepto y naturaleza jurídica 217
3.3.2. Caracteres..... 219
3.4. CONTRATO DE ACCESO A INTERNET 221

3.5. Las obligaciones y cargas de las partes implicadas en la emisión y utilización de la tarjeta de pago en el comercio electrónico 222
3.5.1. Obligaciones y cargas del emisor de la tarjeta 222
3.5.1.1. Cargas del emisor 233
3.5.2. Obligaciones y carga del titular 238
3.5.2.1. Carga del titular 244
3.5.3. Obligaciones y cargas del proveedor de bienes o servicios 249
3.5.4. Obligaciones y carga de la entidad adquirente 260
3.6. Obligaciones de algunos intermediarios en el sistema de pago electrónico mediante tarjeta 263
3.6.1. Obligaciones del proveedor de acceso a Internet 263
3.6.2. Obligaciones del usuario 264
3.6.3. Obligaciones de los prestadores de servicios de certificación 264
3.6.3.1. Obligaciones exigibles a los prestadores de servicios de certificación que expiden certificados reconocidos 266
3.6.3.2. Obligaciones de los prestadores de servicios de certificación que expiden certificados electrónicos 266
3.6.3.3. Obligaciones de los prestadores de servicios de certificación que expiden certificados electrónicos reconocidos 271
3.7. Consideraciones finales 273

CAPÍTULO QUINTO

EL REPARTO DE RIESGOS Y LA ATRIBUCIÓN DE RESPONSABILIDAD POR EL USO FRAUDULENTO DE TARJETA EN EL COMERCIO ELECTRÓNICO

4. INTRODUCCIÓN 279
4.1. La responsabilidad de la entidad emisora de la tarjeta de pago 284
4.1.1. Supuesto de responsabilidad de la entidad emisora 284
4.2. Exención de responsabilidad 295
4.2.1. Cláusula de exención de responsabilidad por extravío o sustracción de la tarjeta de pago 295

4.3. Análisis del Real Decreto Legislativo 1/2007, de 16 de noviembre, de 2007, sobre cláusulas abusivas en relación con los contratos de tarjetas electrónicas de pago 299
4.3.1. Concepto de cláusulas abusivas 300
4.3.2. Requisitos para que una cláusula sea considerada abusiva 301
4.3.3. Nulidad de las cláusulas abusivas en el contrato de tarjeta electrónica de pago 304
4.3.4. Incorporación de las cláusulas abusivas a los contratos de tarjeta de crédito 306
4.4. Medidas adoptadas por las entidades bancarias para minimizar los riesgos y reducir la responsabilidad 317
4.5. Responsabilidad civil del titular de la tarjeta de pago por el uso fraudulento 319
4.5.1. Supuesto de responsabilidad del titular de la tarjeta ante el uso fraudulento en el comercio electrónico 319
4.5.2. Las cláusulas de exención de la responsabilidad del titular de la tarjeta electrónica 325
4.6. Responsabilidad del proveedor de bienes o servicios 329
4.6.1. El cargo indebido o fraudulento mediante el uso de la tarjeta de pago en el comercio electrónico a través de internet 330
4.6.2. La exigencia de la inmediata anulación del cargo 334
4.6.3. La distribución del riesgo por el uso indebido o fraudulento de la tarjeta en el comercio electrónico 336
4.6.4. Análisis del apartado segundo del art. 106 TRLGDCU: el derecho de ejercer la acción correspondiente en reclamación de una indemnización de daños y perjuicios frente al titular 351
4.7. Consideraciones finales 353

CAPÍTULO QUINTO

ESTUDIO PROSPECTIVO PARA LA ELABORACIÓN DE UN MODELO TEÓRICO QUE CONTRIBUYA AL DESARROLLO DEL COMERCIO ELECTRÓNICO EN GUINEA-BISSAU

5. ASPECTOS INTRODUCTORIOS 361
5.1. Datos generales del país 362
A.Demografía y sociedad 366
B.Idiomas hablados 366
5.2. Organizaciones regionales de integración en África Occidental 369
A) La Comunidad Económica de Estados del África Occidental CEDEAO/ ECOWAS 369
B. La Unión Económica y Monetaria del África occidental (UEMOA) 373
C) Organización Africana de Armonización del Derecho Mercantil (OHADA, según sus siglas en francés) 377
5.3. Situación del sistema bancario en Guinea-Bissau 380
5.4. El pago a través de dispositivo móvil en Internet en África 383
1. La utilidad del dispositivo móvil en África 385
2. Componentes de seguridad exigidos en el pago mediante teléfono móvil 386
3. Mecanismos de autenticación de las compras y el pago 387
4. Situación actual de la telefonía móvil en Guinea-Bissau 388
5.5. La situación actual del derecho guineano frente al comercio electrónico 389
5.5.1. La declaración de voluntad por medios electrónicos 391
5.5.2. Perfección de los contratos por medios electrónicos: Momento y Lugar 393
A.Momento de perfección del contrato electrónico 394
B. Lugar de celebración del contrato electrónico 397
5.6. Diagnóstico 399
5.7. Análisis estratégico para el desarrollo del comercio electrónico y el pago mediante tarjeta en Guinea-Bissau (Matriz DAFO) 400
5.7.1. Análisis Interno 400

A.Debilidades....401
B. Fortalezas....404
5.7.2. Análisis Externo....404
A. Oportunidades....405
B. Amenazas....406
5.8. PROCEDIMIENTO DE LA MATRIZ DAFO....408
5.9. La estrategia....410
5.10. Determinación de escenarios....413
5.11. Plan de acción....414
5.12. El pago mediante tarjeta en el comercio electrónico en Guinea-Bissau....421
5.13. Consideraciones finales....423
CONCLUSIONES GENERALES....429
BIBLIOGRAFÍA....441
JURISPRUDENCIA ESPAÑOLA....493
NORMATIVA ESPAÑOLA....501
NORMATIVA COMUNITARIA....507
NORMATIVAS INTERNACIONALY EXTRANJERA NO COMUNITARIA....513
RECURSOS ELECTRÓNICOS....518
GLOSARIO....522

DEDICATORIA

Dedico este trabajo a m i difunta hermana, por su empeño y preocupaciones que ella demostraba siempre en mi formación a lo largo de mi vida estudiantil.

Y en especial a mi madre, hermanas, hermanos, primos, sobrinos, sobrinas, así como a mi querida Elena Barriuso Ríos.

AGRADECIMIENTOS

En primer lugar, me gustaría empezar diciendo que son muchas las personas especiales a las que me gustaría agradecer el hecho de haberme brindado su apoyo, amistad y consejo a lo largo de mi formación. No obstante, me gustaría agradecer, en primer lugar, a mi directora de tesis, Dra. Dª. Teresa Rodríguez de la Heras Ballell (Profesora Titular de Derecho Mercantil de la Universidad Carlos III de Madrid) su apoyo incondicional e interés demostrado en la dirección de esta tesis, así como sus múltiples aportaciones y recomendaciones a lo largo de estos años de la investigación. Gracias también al Profesor Doctor D. Rafael Illescas Ortiz (Catedrático de Derecho Mercantil de la Universidad Carlos III de Madrid), por mantenerme al día con las bibliografías actualizadas.

Deseo expresar mi agradecimiento más sincero al Gobierno de España, en especial a la Agencia Española de Cooperación Internacional y Desarrollo (AECID), por concederme la beca en el año 2005 para cursar el doctorado en la Universidad Carlos III de Madrid. Por lo tanto, extiendo mis gratitudes a todo su personal.

Debo dar las gracias a Dª. Julieta García Morilla (Jefa de la Biblioteca de Derecho de la Universidad de Alcalá de Henares), por haberme ofrecido su ayuda incondicional en la revisión de la tesis y también por permitirme hacer uso de la biblioteca.

Mis agradecimientos para todos los profesores del Departamento de Derecho Privado y Público que me han impartido clases durante mi estancia en la Universidad Carlos III de Madrid, brindándome siempre su orientación con profesionalismo ético en la adquisición de conocimientos y afianzando mi formación como doctorando. En especial, al Profesor Dr. D. Miguel Ruiz Muñoz, al Profesor Dr. D. Jorge Sirvent, a la Profesora Dra. Dª. Lourdes Blanco Pérez-Rubio, a la Profesora Dra. Dª. Marta García Mandalaloniz, Profesor Doctor D. Jorge Feliu y al Profesor Dr. D. Manuel Alba Fernández.

A todos mis amigos y amigas, sin excluir a ninguno, pero en especial al Profesor MS.c. D. Emiliano Carretero Morales, a la Profesora MSc. Dª. Natalia Mato Pacin, Profesora MSc. D. ª Amanda Moreno y a la Profesora Dª. Tatiana, gracias por los apoyos incondicionales que me han brindado a lo largo de esta investigación.

Por último, no quisiera cerrar estas páginas de agradecimientos sin dejar de dar mis gratitudes al Profesor Doctor D. Pascual Correa, de la Facultad de Derecho de la Universidad Central de Las Villas (Cuba).

Para cerrar estas líneas, me gustaría agradecer a mis amigos Ruy Tavares, Sandra Alves, Danilo Lopés, Juelcio Galvâo, Nelson Ca, Domingos Sana, Belarmino Antonio Cabral, Iancuba Intchaso, Antonio(Van), Mamadu Gomes, Mirela y en especial, a D. Álvaro Henrique Barrón (Colombia), por su apoyo incondicional.

ABREVIATURAS

AC	Actualidad Civil
ADC	Anuario de Derecho Civil
AIA	Actualidad Informática Aranzadi
art.	Artículo
arts.	Artículos
ADICAE	Asociación de Usuarios de Bancos, Cajas y Seguros.
AUSBANC	Asociación de Usuarios de Servicios Bancarios
AECE	Asociación Española de Comercio Electrónico
BCEAO	Banco Central de los Estados de África Occidental
BOE	Boletín Oficial del Estado
CC	Código Civil
Cc.	Código de Comercio
Com. E	Comunidad Europea.
C-E	Comercio Electrónico
CE	Comisión Europea
CEE	Comunidad Económica Europea
CES	Comercio electrónico Seguro
CEDECS	Centro de Estudios de Derecho, Economía y Ciencias Sociales
CEDEAO	Comunidad Económica de Estados del África Occidental
CDC	Cuadernos de Derecho y Comercio

CDJ	Cuadernos de Derecho Judicial
CGC	Condiciones generales de contratación
CGPJ	Consejo General del Poder judicial
CNUDMI / UNCITRAL	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional / United Nations Commission for International Trade Law
coord.	Coordinador
coords.	Coordinadores
CVV	Car Verification Value (Código de seguridad)
dir.	Director
dirs.	Directores
DFE	Directiva de Firma Electrónica
disp. adic.	Disposición adicional
DNI	Documento Nacional de Identidad.
DO	Diario Oficial
DOUE	Diario Oficial de la Unión Europea.
ed.	Edición.
Edit.	Editorial.
E-COMMERCE	Electronic commerce (Comercio Electrónico).
ECA	Entidades Certificadoras Autorizadas
EDI	Electronic Data Interchange.
ESC	Estudios sobre Consumo.
FD	Fundamento de Derecho.
FECEMD	Federación Española de Comercio Electrónico y Marketing Directo.
FTP	Protocolo de Transmisión de Ficheros.

HTTP	Protocolo de transferencia en Hipertexto.
https	Protocolo de transferencia en Hipertexto seguro.
HTML	Lenguaje de Marcado en Hipertexto.
ICADE	Instituto Católico de Administración y Dirección de Empresas.
INAP	Instituto Nacional de Administración Públicas.
INTECO	Instituto Nacional de Tecnologías de la Comunicación.
JUR	Jurisprudencia disponible en http://www.westlaw.es
LCC	Ley 7/ 1995, de 23 de marzo, de Crédito al Consumo.
LCGC	Ley 7/1998, de 13 de abril, de Condición General de la Contratación.
LEC	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
LFE	Ley 59/ 2003, de 19 de diciembre, de Firma Electrónica
LCDSFC	Ley 22/2007, de 11 de j ulio, sobre comercialización a distancia de servicios financieros destinados a los consumidores.
LGDCU	Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios
LMISI	Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de Información
LMRSF	Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero,
LMCFE	Ley Modelo de CNUDMI sobre Firmas Electrónicas, 2001
LOCM	Ley 7/1996, de 15 enero, de Ordenación del Comercio Minorista
LRLOCM	Ley 47/2002, de 19 de diciembre, de Reforma de la Ley de Ordenación del Comercio Minorista, para la transposición al ordenamiento jurídico

	español de la Directiva 97/7/CE, en materia de contratos a distancia, y para la adaptación de la ley a diversas directivas comunitarias.
LSP	Ley 16/2009, de 13 de noviembre, de Servicios de Pago.
LSSICE	Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de Información y Comercio Electrónico
MD	Mensaje de Dato
núm.	Número.
OASI	Observatorio Aragonés de la Sociedad de la Información
OCU	Organización de Consumidores y Usuarios
OHADA	Organización Africana de Armonización del Derecho Mercantil
op. cit	Obra citada.
OSI	Oficina de Seguridad del Internauta.
PDDC	Propuesta de Directiva de Derecho de los Consumidores
PIN	Personal identification number (Número de Identificación Personal)
PSC	Prestador de Servicios de Certificación.
PSP	Prestador de Servicios de Pago
p.	Página.
pp.	Páginas.
RCE	Revista de la Contratación Electrónica
RC-E	Revista de Comercio Electrónico
RDBB	Revista de Derecho Bancario y Bursátil.
RDLFE	Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica
REDI	Revista Electrónica de Derecho Informático.
RED	Revista Electrónica de Derecho.
RDI	Revista de Derecho Informático.

RDM Revista de Derecho Mercantil.

RADNI Revista Aranzadi de Derecho y Nuevas Tecnologías.

RDP Revista de Derecho Privado.

RIDI Revista Iberoamericana de Derecho Informático.

RJ Repertorio de Jurisprudencia.

RJN Revista Jurídica del Notariado.

RRCS Revista de Responsabilidad Civil y Seguros.

RTENI Revista de Tecnología y Estrategia de Negocio en Internet.

RSA Rivert, Shamir y Adleman.

S.A. Sociedad Anónima.

SET Secure Electronic Transaction (Transacciones Electrónicas Seguras).

SEPA Single European Payment Area (Área Única de Pagos en Euros)

ss. Siguiente/ Siguientes.

SSL Secure Socket Layer

SWIFT Society for Worldwide Interbank Financial Telecommunications.

Secc. Sección.

SAP Sentencia de la Audiencia Provincial.

SSAP Sentencias de la Audiencia Provincial

STS Sentencia del Tribunal Supremo.

SJPI Sentencia del Juzgado de Primera Instancia.

TCP/IP Transport Control Protocol/ Internet Protocol

TPE Terminales de Pago Electrónico

TPV Terminal de Punto de Venta.

TRLGDUC	Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, que actualiza la Ley 26/1984, de 19 de julio de 1984.
UE	Unión Europea
UEMOA	Unión Económica y Monetaria del África occidental
UOC	Universitat Oberta de Catalunya.
URL	Localizador Uniforme de Recursos.
Vid.	Véase.

RESUMEN

Esta investigación tiene como objetivo determinar la conveniencia de la implementación y el fomento del comercio electrónico en Guinea-Bissau, valorar su viabilidad, identificar los factores que condicionarán esta implantación y proponer un marco regulador adecuado que genere la confianza de los consumidores y proveedores de bienes y servicios.

Para acometer este estudio se realiza un extenso análisis doctrinal, jurisprudencial y legal basado sobre todo en el ordenamiento jurídico español y en el derecho comunitario, que nos permitirá proponer un modelo adecuado para Guinea-Bissau.

El resultado principal del trabajo es un análisis de la situación jurídica, económica y social en Guinea-Bissau a los efectos de la implantación del comercio electrónico que requiere a su vez el fomento de medios de pago electrónicos, en particular, dadas las condiciones del país y las características comerciales y sociales, de las tarjetas de crédito. De este modo, la investigación pretende concluir con la propuesta de un conjunto de medidas basadas sobre todo en la formulación de disposiciones jurídicas que contribuyan al desarrollo de la sociedad de la información y del comercio electrónico seguro.

Además, se propone la reforma del Código Civil y de la Constitución del país, con el objetivo de que se regulen adecuadamente los aspectos relacionados con las nuevas tecnologías de la información y la comunicación y de brindar mayor seguridad jurídica a los entes intervinientes en las operativas de pago mediante tarjeta de crédito en el comercio electrónico.

Palabras claves: autenticación y seguridad; medios de pago electrónico; tarjeta de crédito; confianza de consumidores y usuarios; riesgo; uso fraudulento; responsabilidad; comercio electrónico; obligaciones.

ABSTRACT

This investigation is intended to determine the appropriateness of the implementation and the promotion of electronic commerce in Guinea-Bissau, assess its viability, identify the factors that condition the implementation and propose an appropriate regulatory framework that builds the trust of consumers and suppliers of goods and services. There is an extensive legal, jurisprudential and doctrinal analysis based especially on the Spanish legal system and Community law that will allow us to propose a model suitable for Guinea-Bissau to undertake this study.

The main result of the work is an analysis of the legal, economic and social situation in Guinea-Bissau for the purposes of the implementation of electronic commerce which in turn requires the promotion of electronic means of payment, in particular, given the conditions of the country and the commercial and social characteristics of credit cards. In this way, the research aims to conclude with the proposal of a set of measures based mainly in the formulation of legal provisions which contribute to the development of secure electronic commerce and the information society.

In addition, the reform of the Civil Code and the Constitution of the country, with the aim to properly regulate aspects related to new information and communication technologies and provide greater legal certainty for the entities involved in the operations of the e-commerce credit card payment is proposed.

Keywords: authentication and security; electronic payment means; credit card; confidence of consumers and users; risk; fraudulent use; responsibility; electronic commerce; obligations.

Universidad
Carlos III de Madrid

INTRODUCCIÓN

INTRODUCCIÓN

El desarrollo de las nuevas tecnologías de la información y la comunicación han permitido la creación y el desarrollo de los medios de pago electrónico requeridos para el impulso de la actividad económica y la celebración de transacciones comerciales, bien mediante la implantación de nuevos instrumentos de pago o bien con la adaptación de los medios existentes al nuevo entorno. Se aprecia una reducción de la importancia de los medios de pago tradicionales a la vez que los pagos electrónicos van ganando fuerza, lo que permite una mayor rapidez en la prestación del servicio de pago.

No obstante, como señalan algunos autores, lo que produce oportunidades de mejora en la prestación de un servicio, provoca también riesgos para quien hace uso del mismo. Igualmente, el potencial de las tecnologías no está dando una solución satisfactoria a los problemas que para los consumidores y usuarios plantea el uso fraudulento en las operaciones electrónicas.

Algunas evidencias de falta de seguridad en el uso de las tarjetas de pago en el comercio electrónico (robo de datos personales y bancarios a través de Internet), vienen a demostrar que las nuevas tecnologías de la información y la comunicación hacen surgir riesgos en las operativas de pago con tarjeta de crédito en el comercio electrónico. También cabe señalar como un aspecto problemático el que las entidades emisoras de los medios de pago no garantizan un adecuado nivel de protección a los titulares de estos medios.

No cabe duda de que, en los últimos años, las nuevas tecnologías de la información y la comunicación han revolucionado a nivel internacional amplios sectores del conocimiento y de l as actividades humanas, fomentando el surgimiento de nuevas formas de hac er negocios. En este sentido, cabe resaltar que la implantación del comercio electrónico y el pago mediante tarjeta de crédito o por teléfono móvil a través de Internet es vital para el desarrollo de G uinea-Bissau, y, por lo tanto, es necesario regular esta materia.

Dicha implementación requiere de un esfuerzo coordinado y de acciones integradoras. Por lo que se destaca la necesidad de sensibilizar a los profesionales del Derecho y a los poderes públicos en general, en el fomento de las nuevas tecnologías, y de encarar el comercio electrónico no como una ficción sino como una realidad para impulsar el desarrollo socio-económico de Guinea-Bissau.

El Gobierno debe comprender que la implementación del comercio electrónico supondrá para el país una oportunidad única para el crecimiento económico, ya que se ha convertido en un elemento clave para la realización de negocios a nivel interno y mundial. En este sentido, hay que trabajar en la redacción de proyectos legislativos específicos y de incidencia directa en el comercio electrónico, como instrumentos esenciales para aprovechar esta oportunidad.

Por otro lado, se ha de resaltar que para la implementación del comercio electrónico y el pago mediante tarjeta de crédito en nuestro país, es imprescindible que el Derecho esté presente en dichas actividades con el fin de proteger los intereses de los consumidores y usuarios.

De este modo, cabe plantear el siguiente interrogante: ¿ofrece cobertura el ordenamiento jurídico guineano para regular el comercio electrónico y, en especial, el pago mediante tarjeta de crédito a t ravés de I nternet? Para

resolver la cuestión planteada en la investigación, la hipótesis formulada es que en Guinea-Bissau resultan insuficientes las normas jurídicas reguladoras de los aspectos relacionados con el comercio electrónico y el pago mediante tarjeta de crédito, así como de otros servicios de pago relativos al comercio electrónico, como el uso del teléfono móvil a tal fin. Para demostrar esta hipótesis, tendremos en consideración los presupuestos teórico-doctrinales sobre esta materia y su proyección legislativa, basada sobre todo en el ordenamiento jurídico español y en el derecho comunitario.

Ante la constatación de la escasa relevancia y mínimo conocimiento que el comercio electrónico tiene en Guinea-Bissau, acometemos el presente trabajo planteando los objetivos siguientes:

Objetivo General:

Proponer un diseño doctrinal, jurisprudencial y legal para la implantación del comercio electrónico y del pago mediante tarjeta de crédito, así como de otros servicios de pago que se presenten mejor adaptados al comercio electrónico, que sustente las futuras bases legales reguladoras de la materia en Guinea-Bissau.

Objetivos Específicos:

1. Analizar las diversas modalidades de comercio electrónico y de los medios de pagos electrónicos existentes, con el deseo de aplicar las que creemos más afines al desarrollo de Guinea-Bissau

2. Analizar el riesgo que conlleva el uso de la tarjeta de crédito como medio de pago en el comercio electrónico a través de Internet.

3. Determinar los requisitos necesarios para garantizar un elevado nivel de seguridad en las transacciones electrónicas efectuadas mediante tarjeta de crédito.

4. Analizar los mecanismos tecnológicos (protocolos) que garanticen una correcta manipulación y transmisión de los datos relativos a la tarjeta de pago, con la finalidad de evitar su uso fraudulento en Internet.

5. Determinar quién debe soportar el riesgo de aquellas operaciones llevadas a cabo en Internet, en las que se utilizaron tarjetas de crédito, cuyo número de identificación, aún siendo correcto, no ha sido facilitado por su legítimo titular sino, fraudulentamente, por terceros que, aparentando serlo, lo obtuvieron de manera ilícita e indebida.

6. Elaborar una propuesta que articule el ordenamiento jurídico privado y mercantil de Guinea-Bissau respecto a las normas reguladoras del comercio electrónico y el pago mediante tarjeta de crédito a través de Internet.

Todos estos objetivos son abordados conjuntamente en los capítulos I, II, III, IV y V de esta investigación.

La metodología empleada:

-Amplia y exhaustiva revisión bibliográfica que contribuya al cumplimiento de los objetivos propuestos, a fin de sentar las bases conceptuales y metodológicas de la investigación.

- Análisis de la normativa, tanto española como comunitaria, que regula los aspectos relacionados con el comercio electrónico y los medios de pago electrónico.

-. Análisis de la jurisprudencia que resuelve cuestiones relacionadas con el uso fraudulento de la tarjeta de pago en el comercio electrónico.

- Análisis de las condiciones generales de los contratos de diversas entidades bancarias.

-Finalmente, con la finalidad de investigar el grado de la implementación del comercio electrónico y del pago mediante tarjeta de crédito en Guinea-Bissau, se realizó un estudio basado, sobre todo, en la aplicación de la matriz DAFO[1], método de investigación que se considera apropiado para estudiar la viabilidad de la implantación del comercio electrónico y de los medios de pago electrónicos.

Para establecer una secuencia lógica de la temática de investigación se ha estructurado la misma en cinco capítulos: el primero de ellos está dedicado al comercio electrónico y a los medios de pago electrónicos; el segundo aborda cuestiones relacionadas con la seguridad en los pagos mediante tarjeta de crédito en el comercio electrónico; el capítulo tercero está dedicado al contrato de tarjeta electrónica de pago; en el capítulo cuarto, se abordan las cuestiones relacionadas con el reparto de riesgos y la atribución de responsabilidad civil por el uso fraudulento de tarjeta en el comercio electrónico; y para terminar, en el capítulo quinto, sin duda uno de los más importantes para cumplir el objetivo último de la investigación, se aborda un estudio prospectivo para la elaboración de un modelo teórico que contribuya al desarrollo del comercio electrónico en Guinea-Bissau.

El capítulo primero, dedicado a la delimitación conceptual de las nociones básicas que sustentan la investigación, el comercio electrónico y los medios de pago electrónico, se estructura a su vez en varios epígrafes. En el primero de ellos, se pretende abordar cuestiones tan importantes como el concepto de comercio electrónico, sus modalidades y las diferencias que existen entre ellas; en el segundo se estudia el concepto de pago electrónico; y en el tercero se analiza el concepto de los medios de pago electrónicos.

[1] DAFO (Debilidad, Amenaza, Fortaleza y Oportunidad), es un instrumento de análisis cuantitativo que permite sintetizar informaciones relativas a los factores internos y externos de un sistema, una entidad o una organización.

En cuarto lugar, se estudian las modalidades de los medios electrónicos de pago existentes en la actualidad, partiendo del análisis conceptual, funciones, ventajas e inconvenientes de cada uno de ellos en la operativa de pago electrónico.

El quinto aspecto está dedicado al estudio de la tarjeta de pago, su análisis conceptual y las clasificaciones de tarjetas de pago. Además, se estudia en este capítulo todo lo relacionado con los sujetos intervinientes en la operativa de pago mediante tarjeta en el comercio electrónico, así como el papel de los intermediarios.

En el sexto epígrafe, se analiza la Ley 16/2009, de 13 de noviembre, de Servicios de Pago, que traspone al ordenamiento interno español la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, de servicios de pago en el mercado interior. A continuación, en este capítulo primero, se estudian las ventajas en la utilización de la tarjeta como medio pago en el comercio electrónico a través de Internet, para luego identificar los riesgos en la operativa de pago mediante tarjeta de crédito en el comercio electrónico.

Finalmente, el capítulo primero trata específicamente los tipos de fraude en medios de pago electrónico y sus efectos jurídicos para el consumidor y usuario.

El capítulo segundo que forma esta obra se encuentra estructurado en varios epígrafes:

En el primero de ellos, relativo a la seguridad en las transacciones electrónicas, se pretenden abordar cuestiones tan importantes como la seguridad en el uso del número de las tarjetas a través de Internet.

El segundo aborda las cuestiones relacionadas con los componentes de seguridad exigidos en las transacciones electrónicas seguras.

El tercer epígrafe de este capítulo se dirige al estudio del uso de los métodos criptográficos en las transacciones electrónicas, mediante el uso del número de las tarjetas de pago en el comercio electrónico, partiendo del análisis conceptual y la finalidad de la criptografía, así como sus clases.

Por su parte, el cuarto epígrafe, dedicado a la firma digital y función hash, aborda cuestiones tan importantes como la generación y verificación de la firma digital.

Además, en este segundo capítulo se abordan cuestiones relacionadas con los protocolos de seguridad para la realización de pagos mediante el uso del número de las tarjetas a través de Internet, con especial énfasis en los riesgos que representa el uso del número de la tarjeta en Internet.

Para finalizar el capítulo segundo, se dedica el último epígrafe al análisis sobre las cuestiones relacionadas con la seguridad jurídica en las transacciones electrónicas.

El capítulo tercero analiza los distintos tipos de contratos que conforman el contrato de tarjeta de pago: contrato de emisión de la tarjeta, contrato de pasarela de pago o de aceptación y contrato de acceso a Internet, para luego estudiar las obligaciones que corresponden a cada uno de los sujetos intervinientes en los diversos contratos que conforman el sistema de pago electrónico.

En último lugar, en el capítulo cuarto, se estudian específicamente las obligaciones de los intermediarios en operativas de pago mediante tarjeta en Internet: los prestadores de servicios de certificación y los proveedores de acceso a Internet.

El cuarto capítulo está consagrado al reparto de riesgo y la atribución de responsabilidad civil entre los sujetos intervinientes en la operativa de pago mediante tarjeta en el comercio electrónico en Internet.

En un primer momento, se estudian las cuestiones relacionadas con las atribuciones de la responsabilidad civil en la que puede incurrir la entidad emisora de la tarjeta. Dentro de este epígrafe se han tratado, principalmente, las cuestiones relacionadas con los supuestos de responsabilidad de la entidad emisora y las cláusulas de exoneración de la responsabilidad civil de la entidad emisora por extravío o sustracción de la tarjeta.

Se estudia también, en este capítulo cuarto el Real Decreto Legislativo 1/2007, de 16 de noviembre, de 2007, sobre cláusulas abusivas en los contratos de tarjetas electrónicas de pago, partiendo del análisis conceptual de las cláusulas abusivas, así como los requisitos para que una cláusula sea considerada abusiva, la nulidad de las cláusulas abusivas en el contrato de tarjeta electrónica de pago y la incorporación de dichas cláusulas a los contratos de tarjeta de crédito.

Otro aspecto que se estudia en este capítulo cuarto, son las medidas adoptadas por las entidades bancarias para minimizar los riesgos y reducir la responsabilidad civil.

Igualmente, en este capítulo, se aborda el análisis de la responsabilidad civil del titular de la tarjeta, los supuestos de responsabilidad del titular de la tarjeta ante el uso fraudulento en el comercio electrónico y las cláusulas de exoneración de la responsabilidad civil del titular de la tarjeta.

Por su parte, en el apartado sexto de este mismo capítulo, se estudia la responsabilidad civil del prestador de bienes o servicios.

En el séptimo apartado de este capítulo, se estudia el cargo fraudulento o indebido mediante la utilización del número de una tarjeta de pago, poniendo especial atención en la exigencia de la inmediata anulación del cargo. Asimismo, se analiza la distribución del riesgo por el uso indebido o fraudulento de la tarjeta en el comercio electrónico.

Y por último, para finalizar este capítulo cuarto, se abordan cuestiones relacionadas con el derecho a ejercer la acción correspondiente en reclamación de una indemnización de daños y perjuicios frente al titular (art.106.2 TRLGDCU).

Finalmente, en el quinto y último capítulo, se aborda un estudio prospectivo para la elaboración de un modelo teórico que contribuya al desarrollo del comercio electrónico en Guinea-Bissau. Este capítulo se divide a su vez en varios epígrafes:

En una primera parte, se exponen los datos generales de Guinea-Bissau con el objetivo de comprender de qué país estamos hablando. Se incluyen también algunas de las características y elementos del país (clima, situación geográfica, demografía y sociedad) que pueden condicionar su desarrollo.

En una segunda parte, se analizan las organizaciones regionales de integración en África Occidental, de las que Guinea-Bissau es miembro. Dentro de este capítulo quinto se expone la situación del sistema bancario en Guinea-Bissau. Además, se hace un análisis de la importancia del pago por móvil en África y su papel en la bancarización de la población africana.

A continuación, se estudia la situación del derecho guineano frente al comercio electrónico.

Y por último, para cumplir con uno de los objetivos de este trabajo, se abordan las cuestiones relacionadas con el análisis estratégico para el

desarrollo del comercio electrónico y el pago mediante tarjeta (Matriz DAFO) en Guinea-Bissau.

Finalmente, cabe concluir que hemos analizado el ordenamiento jurídico español porque cuenta en la actualidad con un conjunto de importantes disposiciones (que transponen el derecho comunitario) tendentes a regular con carácter general el pago mediante tarjeta en el comercio electrónico y en base a eso hemos propuesto algunas modificaciones que deben servir como punto de partida para el desarrollo de las futuras normativas jurídicas en Guinea-Bissau.

En este mismo sentido, algunas de las razones por las que hemos elegido el derecho español como referencia a lo largo de esta investigación son las siguientes:

- A nivel legislativo, en la actualidad España cuenta con una normativa de servicios de pago (LSP) que recoge, de forma concluyente y obligatoria, el régimen de responsabilidades y obligaciones de las partes intervinientes en la operativa de pago electrónico.

- España es uno de los países de la eurozona en el que el nivel de desarrollo del comercio electrónico y de los diversos medios de pago electrónico sigue creciendo. Además, el número de los internautas o de consumidores que navega y compra por Internet va en aumento.

- Además, tanto la legislación española, como la doctrina, y la jurisprudencia han construido una línea de pensamiento que creemos es imprescindible como guía para la implantación del comercio electrónico en nuestro país.

- El interés demostrado por el autor en la elección y la consideración del ordenamiento jurídico español se debió al hecho de haber terminado un Master Oficial en Derecho Privado en esta Universidad

Cerrando estas líneas introductorias, cabe resaltar que se han desarrollado un conjunto de conclusiones sobre los diversos aspectos de la implantación del comercio electrónico y el pago mediante la tarjeta de crédito en Guinea-Bissau. En ellas se intenta realizar un aporte para la solución de los diferentes problemas que puede acarrear la implantación del comercio electrónico en nuestro país.

Tras la exposición de las conclusiones generales del presente trabajo, la investigación concluye con la relación de las referencias bibliográficas citadas y de la jurisprudencia y legislación consultada para su elaboración.

Universidad
Carlos III de Madrid

CAPÍTULO PRIMERO

EL COMERCIO ELECTRÓNICO Y LOS MEDIOS DE PAGO ELECTRÓNICOS: ANÁLISIS DEL PAGO CON TARJETA EN EL COMERCIO ELECTRÓNICO

CAPITULO I.

EL COMERCIO ELECTRÓNICO Y LOS MEDIOS DE PAGO ELECTRÓNICOS: ANALISIS DEL PAGO CON TARJETA EN EL COMERCIO ELECTRÓNICO

I. Precisiones introductorias

Resulta interesante destacar la tesis sostenida por algún autor, que destaca que el comercio electrónico "es un nuevo soporte pero también un nuevo mercado o ámbito de relaciones negóciales"[2]. Este mismo autor resalta que "la expresión comercio electrónico, de uso hoy tan extendido, no es unívoca sino que bajo su manto se organizan identidades, actividades y relaciones contractuales susceptibles de diverso tratamiento jurídico.

Del mismo modo resulta interesante resaltar el criterio sostenido por algún autor, tras sostener que "a medida que las relaciones sociales y la actividad económica han ido migrando, en un proceso constante e imparable, al espacio digital, la cuestión de s u regulación ha venido implicando una previa apreciación de l a suficiencia y la adecuación de las reglas preexistentes al nuevo entorno. Porque el verdadero reto que representa la sociedad de la información, la emergencia y consolidación de Internet, la penetración de las tecnologías de información y comunicación en las relaciones sociales y las actividades económicas es precisamente la duplicación del espacio. Junto al espacio analógico o n atural emerge un

[2] ILLESCAS ORTIZ, Rafael. *Derecho de la contratación electrónica*. 2. ª ed. Cizur Menor (Navarra): Aranzadi, SA, 2009, p. 20.

nuevo espacio, el espacio digital, (…)[3]. Es decir, dicha autora, sostiene que los medios electrónicos representan la aparición de un nuevo espacio.

Los medios electrónicos de pago constituyen un elemento imprescindible para el desarrollo del comercio electrónico y, en general, de la actividad económica en ese nuevo espacio. Estos medios adquieren gran importancia por la unión que se produce entre operadores de telecomunicaciones y entidades financieras para el desarrollo de medios de pago específicos que permitan dar respuesta a las necesidades de una contratación que se produce sin la presencia física simultánea de las partes.

Una red abierta como Internet[4] no sólo supone una fuente para adquirir o transmitir información. También es un gran mercado en el que se pueden adquirir bienes o servicios. Es de destacar, en este sentido, que el uso de los medios de pago electrónicos en Internet plantea una serie de cuestiones que requieren, lógicamente, una respuesta no solo técnica sino también jurídica. Cuestiones como la necesidad de proporcionar seguridad en la realización de pagos a través de redes electrónicas, la lucha contra el fraude en medios

[3] RODRÍGUEZ DE LAS HERAS BALLELL, Teresa «Intermediación en la Red y responsabilidad civil. Sobre la aplicación de las reglas generales de la responsabilidad a las actividades de intermediación en la Red», en *Revista Española de Seguros*, núm. 142, 2010, pp. 217-259.; también publicado en VV.AA., I *Congreso sobre las Nuevas Tecnologías y sus repercusiones en el seguro: Internet, Biotecnología y Nanotecnología*, Madrid: Fundación Mapfre, 2011, pp. 13-50.

[4] Cabe destacar, que Internet es considerada como infraestructura de redes a escala mundial que se conecta a la vez a todo tipo de computadores. Desarrollado originariamente para los militares de Estados Unidos, después se utilizó para el gobierno, la investigación académica y comercial y para comunicaciones; El carácter abierto que presenta Internet permite la interoperabilidad y la ventaja de participar en un amplio mercado junto con la posibilidad de integrar un producto o proceso con otro; vid. BARRIUSO RUIZ, Carlos. *La contratación electrónica*, 3. ª ed. Madrid: Dykinson, 2006, pp. 63 y ss; vid. HORTAL I VALLVÉ, Joan; ROCCATAGLIATA, Franco y VALENTE, Piergiorgio. *La fiscalidad del comercio electrónico*. Valencia: Editorial CISS, S.A., 2000, p. 264; Según pone de relieve el Profesor ILLESCAS ORTIZ, tras referirse el surgimiento de Internet, se está "en presencia de alteración contractual de similar importancia a la que se produjo con la sustitución de la tabla o tablilla de piedra o barro por el papiro y la del pergamino", ILLESCAS ORTIZ, R. «El comercio electrónico: fundamentos de derecho y el principio de equivalencia funcional», en *Boletín de Inflación y Análisis Macroeconómico,* núm. 56, mayo199, pp. 2913 y ss. PASTOR SEMPERE, Mª. Del Carmen. *Dinero electrónico*. Prólogo de Luis Fernández de la Gándara. Madrid: Editoriales de Derecho Reunidas, S. A., 2003, p. 23, nota 8.

de pago o la necesidad de garantizar, cuando ello sea posible, la privacidad en las operaciones.

El objetivo de este capítulo es analizar las diversas modalidades de comercio electrónico y de los medios de pagos electrónicos existentes, con el deseo de aplicar las que creemos más afines al desarrollo de Guinea-Bissau.

1.1. Comercio electrónico: concepto y modalidades

1.1.1. Concepto de comercio electrónico

Para acometer el estudio de los medios de pago electrónicos es preciso, en primer lugar, definir en qué consiste el comercio electrónico, también frecuentemente referido como e-commerce (*electronic commerce* en inglés) y cuáles son las modalidades en las que podemos clasificarlo.

Para definir el comercio electrónico hemos de tener en cuenta una serie de conceptos que definen diferentes autores[5] y normativas, tanto internas como internacionales.

[5] Según sostiene MARTÍNEZ NADAL, el comercio electrónico "es todo intercambio de datos por medios electrónicos, esté relacionado o no con la actividad comercial en sentido estricto", en MARTÍNEZ NADAL, Apol-lonia. *Comercio electrónico, firma digital y autoridades de certificación*. Prólogo de Guillermo Alcover Garau. Madrid: Civitas, 1998, p.25; vid. ALONSO CONDE, Ana Belén. *Comercio electrónico: antecedentes, fundamentos y estado actual.* Madrid: Dykinson S.L., 2004, p.15; según la define RICO CARRILLO, como "toda forma de transacción comercial realizadas por medios electrónicos, la cual incluye los entornos cerrados-como el EDI(Intercambio electrónico de Dato)- y otros medios electrónicos de comunicación, como télex, teléfono, fax o el uso de la TV digital…"; en este mismo sentido, GARCÍA DEL POYO la define como, "intercambio electrónico de datos e informaciones correspondientes a una transacción de contenido económico, no limitándose únicamente a las transacciones a través de Internet, sino también abarca aquellas que utilizan medios como fax, el EDI, u otros mecanismos similares", GARCÍA DEL POYO, Rafael, "Aspectos mercantiles y fiscales del e-business", en ECHEVARIA SAÉNZ, Joseba Aitor (coord.). *El comercio electrónico*. Madrid: EDISOFER S.L., 2001, p. 491; VICENTE CHULÍA, Fco. *Introducción al Derecho Mercantil.* 19. ª ed. Valencia: Tiran lo Blanch, 2006, p. 827.

Al respecto, la Organización Mundial del Comercio (OMC) define al comercio electrónico como «la producción, publicidad, venta y distribución de productos a través de las redes de telecomunicaciones»[6].

Por su parte, la Ley Modelo sobre Comercio Electrónico, aprobada por la Asamblea General de la ONU en su 29º periodo de sesiones, de 28 de mayo a 14 de junio de 1996, Nueva York (en adelante Ley Modelo)[7] no recoge una definición de comercio electrónico. Sin embargo, en la guía elaborada por este órgano para la incorporación de esta ley al derecho interno, se establece que el comercio electrónico comprende todas aquellas transacciones comerciales que se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación, en los que se usan medios de comunicación y almacenamiento de información sustitutivos de los que usan papel.

Hay quien señala, que la expresión «comercio electrónico» abarcaría todas "aquellas facetas de la actividad económica cuando éstas se inician, se desenvuelven o se concluyen a través de medios de telecomunicación a distancia"[8]. Mientras que para otros autores sería más adecuado utilizar una definición, considerada como más estricta, de comercio electrónico, como "toda forma de comercio en la cual se utilizan las redes de ordenadores

[6] Organización mundial del comercio. *Estudio especial de la OMC sobre el comercio electrónico.*[En línea] disponible en Internet: http://www.wto.org/spanish/tratop_s/ecom_s/special_study_s.pdf (última consulta, 16 de julio de 2012), p. 1.

[7] Naciones Unidas: Ley Modelo CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 [En línea] Disponible en Internet:http://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf(última consulta, 23 de mayo de 2012).

[8] RODRÍGUEZ DE LAS HERAS BALLELL, T. *El régimen jurídico de los mercados electrónicos cerrados (e-Marketplaces*. Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2006, p. 32.

como medio de comunicación entre los diferentes agentes implicados"[9]. Sin embargo, no creemos que dicha definición sea más estricta.

Resumiendo, podemos definir el comercio electrónico como un conjunto de actividades mercantiles que incluyen tanto actividades comerciales como acciones de mercadeo, de bienes tangibles o intangibles, siempre que éstas se produzcan por vía electrónica, sobre todo en la redes de comunicación, como es el caso de Internet. Es decir, el comercio electrónico se puede entender como cualquier forma de transacción o intercambio de información comercial (compraventas de bienes y prestación de servicios realizados entre empresarios, o bien entre empresarios y consumidores) basada en la transmisión de datos en la red abierta de Internet[10].

Por último, se ha de hacer hincapié en que el comercio electrónico no es sólo compra electrónica, sino que abarca la producción, publicidad, venta y distribución de productos a través de las redes de comunicación, o sea

[9] VILA SOBRINO, José Antonio. "Marco general del comercio electrónico", en GOMÉZ SEGADE, José Antonio (dir.). *Comercio electrónico en Internet*. Madrid: Marcial Pons, 2001, p.51.

[10] Véanse VASQUEZ CALLAO, Enrique; BERROCAL COMENAREJO, Julio. *Comercio electrónico. Material para Análisis.* Madrid: Centro de publicaciones, Secretaria General Técnica, Ministerio de Fomento, 2000, p.1; PARDO, Fernando. "Implantación social. Situación del comercio electrónico en España", en GOMÉZ SEGADE, José Antonio (dir.). *Comercio electrónico en Internet*. Madrid: Marcial Pons, 2001, p.85 y ss; GARCÍA MÁS, Francisco Javier. *Comercio y firma electrónicos. Análisis jurídico de los servicios de la sociedad de la información.* 2.ª ed. Valladolid: Edit. Lex Nova, 2004, p. 31; para el profesor DOMÍNGUEZ DUELMO, se puede entender el comercio electrónico como "las transacciones comerciales electrónicas (compraventas y prestaciones de servicios), así como las negociaciones previas y ulteriores a las mismas" DOMÍNGUEZ DUELMO, Andrés. "La contratación electrónica con consumidores", en MATA y MARTÍN, Ricardo M (dir.*). Los Medios electrónicos de pago. Problemas jurídicos*. Granada: comares, 2007, p. 71; según sostienen los autores GÓMEZ VIETES y VELOSO ESPIÑEIRA, se puede definir el comercio electrónico como "la automatización mediante las tecnologías de información de los intercambios de información asociados a la compra de bienes y servicios y el pago de los mismos", en GÓMEZ VIETES, Álvaro; VELOSO ESPIÑEIRA, Manuel. *Economía digital y comercio electrónico.* Santiago de Compostela: EDITA Escuela de Negocios Caixa Nova-Tórculo Ediciones, S.L., p. 77; vid. GUISADO MORENO, Ángela. *Formación y perfección del contrato en Internet*. Prólogo de Leopoldo J. Porfirio Carpio. Madrid: Marcial Pons, Ediciones jurídicas y Sociales, S. A., 2004, p. 59; vid. PASTOR SEMPERE, Mª. C. *Dinero*…op., cit., p. 24; vid. BURGO PUYO, Andrea. *El consumidor y los contratos en Internet. Colombia:* Universidad Externado de Colombia, 2007, p. 19.

cualquier forma de transacción o intercambio de información comercial, basada en la transmisión de datos sobre redes de comunicación.

A continuación, estudiaremos las distintas modalidades de comercio electrónico existentes.

1.1.2. Modalidades de comercio electrónico

El comercio electrónico se encuentra en una fase de expansión gracias a Internet. Es por esto que el interés de estudiar las modalidades de comercio electrónico se encuentra en el deseo de aplicar esta modelización al estado de desarrollo de Guinea-Bissau y así entender las necesidades de normativas y de tecnología.

En este sentido, se puede clasificar el comercio electrónico en diferentes tipos según el objetivo que persigamos:

1.1.2.1. *Por cómo se realiza el contrato*

A. Comercio electrónico directo

Se trata de la compra de un bien inmaterial, contenido en soporte digital cuya entrega y el pago se efectúan on line[11]. O sea, tanto la oferta y la

[11] Véanse, ILLESCAS ORTIZ, Rl. *Derecho de la…* op., cit., p. 23; DOMÍNGUEZ LUELMO, Andrés."La contratación electrónica y la defensa del consumidor", en ECHEVARIA SAÉNZ, Joseba Aitor (coord.). *El comercio electrónico*. Madrid: EDISOFER S.L., 2001, p. 34; APARICIO VAQUERO, Juan Pablo. *Internet…op.cit.,* p.179; HARGAIN, Daniel. "Ejecución del contrato por medios electrónicos", en FERRER, Alicia; HARGAIN, Daniel; y CAFFERA, Gerardo (coords). *Comercio electrónico. Análisis jurídico multidisciplinario*. Buenos Aires: Euros Editores S.L., 2003, pp.161-171, en especial pp.163 y ss; DEL PESO NAVARRO, Emilio. *Servicios de la sociedad de la información. Comercio electrónico y protección de datos*. Madrid: Ediciones Díaz de Santos, S.A., 2003, p. 20; vid. PATRONI VIZQUERRA, Úrsula. *Apuntes sobre comercio electrónico*. [En línea] Disponible en Internet: http://www.teleley.com/articulos/art-apuntes_comercio_electronico.pdf (última consulta, 17 de agosto de 2012); vid. ILLESCAS ORTIZ, R. *Derecho de la contratación electrónica*. Cizur Menor (Navarra): Civitas, 2009, pp. 339-340; vid. HORTAL I VALLVÉ, Joan; ROCCATAGLIATA, Fco. *La fiscalidad...*op., cit., p. 23, nota 21; GUISADO MORENO, Á.: *Formación y perfección…*op., cit., pp. 67 y ss; DE MIGUEL ASENSIO, Pedro Alberto. *Derecho privado de Internet*. Madrid: Civitas, 2002, pp. 344 y ss. MATEU DE ROS, Rafael. "Principios de la contratación electrónica. La Ley de servicios de la sociedad de la información y de comercio electrónico", en MATEU DE ROS, Rafael; LÓPIZ-MONIS

aceptación como la entrega de bienes o servicios intangibles, se producen electrónicamente. Por ejemplo, aquellos servicios relacionados con la compra de un software, billete de avión, música, videos, libros electrónicos, juegos de ordenador e información, entre otras. En este sentido, se ha de subrayar que el uso de esta modalidad de comercio electrónico directo permite al consumidor adquirir bienes sin la necesidad de desplazarse físicamente.

Es una modalidad de comercio electrónico que aprovecha de las potencialidades de Internet y sus tecnologías asociadas, facilitando no sólo que los bienes o servicios se contraten y suministren a través de la red, sino también que el pago se efectué dentro del propio entorno electrónico en que las partes interactúan[12]. Es decir, el desarrollo de las fases negóciales se produce en Internet, por lo que las partes podrán prescindir de los medios de distribuciones tradicionales y así reducir los costes de las transacciones comerciales. Estas son las ventajas que representa el comercio electrónico directo[13].

B. Comercio electrónico indirecto

Es aquel en el que la compra de bienes materiales o tangibles o la contratación de servicios se realiza por vía electrónica, mientras que la entrega de bienes o la prestación de servicios se efectúa por los medios tradicionales, entre los que se encuentran el correo postal o los servicios de mensajería y los medios de transporte (marítimo, aéreo, terrestre) y logística, es decir, fuera de línea (off line)[14], ya que no es factible su entrega o su

GALLEGO, Mónica. *Derecho de Internet.* Prologo de Carlos López Blanco. Cizur Menor (Navarra): Aranzadi, S.L., 2003, p. 106.

[12] Vid. MADRID PARRA, Agustín. "Seguridad en el comercio electrónico", en ORDUÑA MORENO, Francisco J. (dir.*). Contratación y comercio electrónico*. Valencia: Tirant Lo Blanch, 2003, p.144.

[13] Ibídem, p. 67 y ss.

[14] Vid. DOMÍNGUEZ LUELMO, A. "La contratación…"*op., cit*., p. 34; FERNÁNDEZ DOMINGO, Jesús Ignacio. "Algunas notas acerca de la contratación y el comercio

prestación en la red. En este mismo sentido, hay quienes lo consideran como un "comercio electrónico imperfecto en el que todas las fases de la contratación se realizan de manera electrónica, excepto el pago y la entrega de la cosa que siguen sistemas tradicionales"[15]. Criterio que consideramos erróneo, ya que el pago puede ser electrónico.

Por último, cabe señalar que el comercio electrónico indirecto, o las operaciones "off line", son aquellas en las cuales la contratación de bienes o servicios y la publicidad de los mismos se realiza por vía telemática, de modo que se empleará Internet para contratar la operación, pero la prestación –entrega del bien o realización del servicio- y, en ocasiones, la contraprestación –el pago--, se realizarán por cauces tradicionales, pues dependerá del objeto contratado que el pago sea contra reembolso o a través de medios electrónicos[16].

Es importante señalar que, en este tipo de modalidad de comercio electrónico, no es de carácter obligatorio efectuar el pago fuera de línea (off

electrónico", en ORDUÑA MORENO, Francisco Javier (dir.). *Contratación electrónica y comercio electrónico*. Valencia: Tirant Lo Blanch, 2003, p. 253; ALONSO CONDE, A. B. *Comercio…*op., cit., p. 26; APARICIO VAQUERO, J. P. *Internet…op., cit.,* p.179; vid. FELIU ALVAREZ DE SOTOMAYOR, Silvia. *La contratación internacional por vía electrónica con participación de consumidores. La elección entre la vía judicial y la vía extrajudicial para la resolución de conflictos.* Granada: Comares, 2006, p. 9; vid. HORTAL I VALLVÉ, J; ROCCATAGLIATA, F. y VALENTE, P. *La fiscalidad...*op., cit., p. 23, nota 21; vid. GUISADO MORENO, Ángela. *Formación…*op., cit., p. 68; PLAZA PENADÉS, Javier. "Contratación electrónica y pago electrónico en el derecho nacional e internacional", en ORDUÑA MORENO, Francisco Javier. (dir.*). Contratación y comercio electrónico*. Valencia: Tirant Lo Blanch, 2003, p. 451

[15] DEL PESO NAVARRO, E. *Servicios de la…op., cit.,* p. 22; FELIU ÁLVAREZ DE SOTOMAYOR, S. *La contratación…*op., cit., pp. 9 y ss.

[16] Suscribiendo textualmente la tesis sostenida por el Profesor MADRID PARRA, tras señalar que, "aun cuando un contrato se haya celebrado por medios electrónicos, a la hora de su consumación el cumplimiento de la obligación del pago se puede llevar a cabo por medios tradicionales o por los más modernos que facilitan las nuevas tecnologías, pero prácticamente supondrá, en la mayoría de los casos, una distorsión no acompasada con los medios tecnológicos utilizados para la fase de perfección del contrato", MADRID PARRA, A. "Seguridad en el…*op., cit.,* p. 144. DE MIGUEL ASENSIO, P. A. *Derecho privado…*op., cit., p. 344.

line)pues se puede contratar y pagar directamente on line, pero la entrega debe ser realizada físicamente, porque se trata de bienes materiales.

C. Distinción entre el comercio electrónico directo y el comercio electrónico indirecto

Las diferencias existentes entre estas dos modalidades de comercio electrónico se pueden resumir en las siguientes: en el *comercio electrónico indirecto (off line)*[17] la oferta y la aceptación se producen electrónicamente, mientras que los bienes o servicios se entregan físicamente. Esta modalidad de comercio electrónico puede ofrecer inicialmente mayor confianza a los consumidores y usuarios, por ejemplo realizando el pago contra reembolso, pero limita enormemente las posibilidades del sistema[18].

En cambio, en *el comercio electrónico directo (on line),* se produce en línea tanto la oferta y aceptación como la entrega de bienes o servicios intangibles y el pago de los mismos[19]. Por ejemplo, compra de un software, música, videos, libros electrónicos, billetes electrónicos, antivirus y juegos de ordenador.

En este sentido, se ha de resaltar que la generalización de esta modalidad de comercio electrónico depende de la confianza en la seguridad del mismo, especialmente entre sujetos desconocidos y geográficamente distantes[20].

1.1.2.2. *Según los entes intervinientes*

Siguiendo el criterio sostenido por algunos autores, "el comercio electrónico ha dado un importante paso evolutivo con su aplicación en

[17] Ibídem, *op., cit.,* p.265.
[18] DOMÍNGUEZ LUELMO, A. "La contratación…"*op., cit.,* p. 71.
[19] Vid. HORTAL I VALLVÉ, J; ROCCATAGLIATA, Franco y VALENTE, P. *La fiscalidad del…op., cit.,* pp.264-265.
[20] Ibidem, *op., cit*., p.72.

internet y ha desarrollado en la web características muy diferentes al tipo de comercio electrónico que desde hace muchos años se viene desarrollando entre organizaciones"[21] En la actualidad existen cuatro modalidades de comercio electrónico claramente diferenciadas según los participantes[22], pero en los últimos años se ha generalizado la tendencia a utilizar estos acrónimos para definir nuevos modelos de negocio o fenómenos sociales (por ejemplo, P2C Lending para describir modelos de financiación *"Person To Company*" de las corrientes de Crowdfunding).

A. El comercio electrónico entre empresas B2B (Business to Business)

Es el que genera un mayor volumen de transacciones[23]. Está establecido hace años, usando en particular el EDI (Electronic Data Interchange) sobre redes privadas o de valor añadido. Este tipo de comercio electrónico se refiere a la compra y venta de productos o servicios entre empresas[24].

[21] ESCOBAR ESPINAR, Modesto. *El comercio electrónico. Perspectiva presente y futura en España.* Madrid: Fundación Retevisión, 2000, p 22.

[22] RODRÍGUEZ DE LAS HERAS BALLELL, T. *El régimen jurídico…*op., cit., pp. 40 y ss.

[23] ESCOBAR ESPINAR, M. *El comercio…op., cit.,* p.33; APARICIO VAQUERO, Juan Pablo. *Internet y comercio electrónico*. Salamanca: Ediciones Universidad de Salamanca, 2002, p.179; GÓMEZ VIETES, Á y VELOSO ESPIÑEIRA, M. *Economía digital…op., cit.,* pp. 83 y ss; a juico de RAMOS SUARES, el comercio electrónico entre empresarios incluye "…todas aquellas actividades que supongan transacciones o envío de información en procesos comerciales con los proveedores, socios o canales, como pueden ser pedidos, pagos, servicios básicos de adquisición, sistemas de ayuda a la distribución, gestión de la logística etc. Su objetivo principal es la automatización de la gestión empresarial y la eliminación de costes asociados como la facturación, el desplazamiento, gastos en papel, comunicación, etc. La eliminación de estos costes, según varios estudios publicados, permitiría multiplicar los beneficios de la mayoría de las empresas y ofrecer al empresario un mayor control de sus procesos", en R AMOS SUARES, Fernando. *El comercio electrónico: la seguridad técnica y jurídica.* [En línea] Disponible en Internet:http://www.masterdisseny.com/master-net/legalia/0006.php3 (última consulta, 6 de julio de 2012); RICO CARRILLO, M*. Comercio electrónico…op., cit.,* p.41.

[24] ALONSO CONDE, A. B. *Comercio electrónico*…op., cit., p. 16; HORTAL I VALLVÉ, J; ROCCATAGLIATA, Fco y VALENTE, P. *La fiscalidad del…op., cit.,* p.24.

B. El comercio electrónico empresa-consumidor (business to consumer B2C)

Consiste en la compra y venta de productos o de servicios a través de medios electrónicos como Internet[25], y se ha expandido con el desarrollo de la Word Wide Web (www)[26], donde hay gran cantidad de galerías, centros comerciales y tiendas virtuales que operan en Internet.

[25] Vid. ESCOBAR ESPINAR, M. *El comercio*…op., cit., pp.127; VILA SOBRINO, J.A. "Marco general…"*op., cit.,* p. 54 y ss; VASQUEZ CALLAO, E. y BERROCAL COMENAREJO, J. *Comercio electrónico…*op., cit., p.1 y ss; *ibídem*, pp. 121 y ss; vid. ESCOBAR ESPINAR, M. *El comercio…op., cit.,* pp. 35 y ss.

[26] El inventor de la *web* fue el científico británico Tim Berners-Lee, quien encontró en 1989 la forma de insertar vínculos de un texto en otro documento, comenzando a utilizarse popularmente en 1992; La Word Wide Web (WWW)*:* es definida como "tela de araña mundial", que viene siendo una forma de recibir, presentar y descubrir informaciones multimedia en Internet, es la herramienta servidor que junto con un programa navegador cliente, facilita y populariza el uso de Internet. Está formado por servidores web repartidos por la red que dan acceso a información y servicios, que pueden gestionarse con buscadores como Google, Yahoo, Alta vista, Infoseek, Webcawler, etc., a través de palabras clave, o por tema. Es un sistema de información de Internet, donde los documentos hipertexto contienen palabras que se pueden designar como enlaces o vínculos *(link)* a otros documentos hipertexto que contienen información relevante.

También es definida detalladamente en la Enciclopedia Encarta, como "una colección de ficheros, denominados lugares de Web o páginas de Web, que incluyen información en forma de textos, gráficos, sonidos y vídeos, además de vínculos con otros ficheros". Los ficheros son identificados por un localizador universal de recursos que específica el protocolo de transferencia, la dirección de Internet de la máquina y el nombre del fichero (por ejemplo, un url podría ser http://www.encarta.es/msn.com.

Los programas informáticos denominados exploradores--como Navigator de Netscape, o Internet Explorer, de Microsoft--utilizan el protocolo http para recuperar esos ficheros. Continuamente se desarrollan nuevos tipos de ficheros para la WWW, que contienen por ejemplo animación o realidad virtual (vrml)".

Las páginas web, comerciales o no, pueden ser un elemento más de una empresa, o bien pueden ser la empresa en sí misma. Algunos sitios comerciales se han creado para ampliar las actividades de empresas que funcionan normalmente en el mundo real, por lo que, al ser complementarios de aquéllas, están sometidos al régimen de la misma, tanto en controles, jurisdicción, fiscalidad, etc...

Muchas empresas abren su sitio web con los fines de mejorar su credibilidad con la proyección de una imagen actualizada y más sólida; promocionar sus productos y servicios; anunciar en más mercados con menores gastos; mejorar el servicio al cliente; ofrecer documentación sin burocracia; realizar investigaciones de mercados extranjeros; usar el correo electrónico como una herramienta de mercadeo y de comunicación con los clientes, entre otras", HERNANDEZ FERNÁNDEZ**,** L. *Momento* y…op., cit., p. 23; sobre este aspecto véanse BARRIUSO RUIZ, C., *La contratación…op., cit.,* pp. 84 y ss; DELGADO KLOOS, Carlos; FERNÁNDEZ PANADERO, M. ª Carmen "Fundamentos de la Word wide web.

Dada la importancia para nuestra investigación, debemos definir, en primer lugar, el denominado prestador de servicios de la sociedad de la información, definido por el inciso c) del Anexo de la LSSICE como "persona física o jurídica que proporciona un servicio de la sociedad de la información"[27].

En segundo lugar, al consumidor o usuario como: "la persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información" (inciso d) del anexo de la LSSICE). Por su parte, el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU) lo define en su art. 3 como: "las personas físicas o jurídicas que actúan en un ámbito ajeno a una actividad empresarial o profesional".

A continuación, hacemos uso del informe de estudio sobre comercio electrónico B2C 2011 en España. Según este informe elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), sobre volumen de ventas por modelo de negocios de comercio electrónico entre empresa y consumidor (B2C) en España, el

---

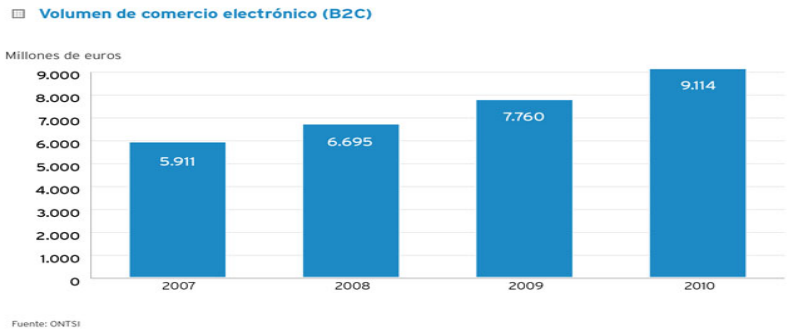
Nuevos formatos. Nuevos modelos de negocio", en ILLESCAS ORTIZ, R. (dir.). *Derecho del comercio electrónico*. Madrid: Editorial la Ley, 2001, pp. 39 y ss; DE MIGUEL ASENSIO, Pedro Ángel. *Derecho Privado de Internet*, 2. ª ed., Madrid: Civitas, 2000, pp. 29-30; PASTOR SEMPERE, Mª. Del C. *Dinero*…op., cit., pp. 26-27.

[27] Véanse, GRAMUNT FOMBUENA, Mª. DOLOR, "El estatuto jurídico de los prestadores de servicios de la sociedad de la información". *en* BARRAL VIÑAL, Inmaculada (coord.). *La regulación del comercio electrónico.* Madrid: Dykinson, 2003, p. 17, este sostiene que los servicios que prestan los prestadores, son todo los servicio prestado normalmente a titulo oneroso, a distancia, por vía electrónica y a petición individual del interesado; siguiendo la tesis de RODRÍGUEZ DE LAS HERAS BALLELL, T. El *régimen jurídico de los…*op., cit., pp.129 y ss, en la que sostiene que en la LSSICE, no existe una claridad a la hora de definir los términos prestador de servicios y destinatario. Y que el legislador no diferencia adecuadamente la prestación de servicios de comunicación y la prestación de servicios comerciales, que utilizan la red de telecomunicaciones como medio de transmisión de la información, por lo tanto, el término o vocablo destinatario del servicio y el de prestador se hacen especialmente confusos; ILLESCAS ORTIZ, R. «Claroscuro con patitos. De nuevo sobre la legislación proyectada en materia de contratación electrónica». *RCE,* núm.27, mayo 2002, pp. 3-26.

comercio electrónico en 2010 ha generado una cifra de negocio que supera los 9.100 millones de euros, incrementando en un 17,4% los 7.760 millones de euros del año anterior[28].

La estimación de la cifra de negocio que supone el comercio electrónico en 2010 se obtiene de computar el número total de compradores on-line (que se estiman en 11 millones a comienzos de 2010) por el gasto anual medio por internauta comprador (831€).

Observen el grafico 1 sobre volumen de comercio electrónico entre empresario y consumidor (B2C) en España.



Fuente: ONTSI

Mientras que, en 2011, el mercado B2C en España ha crecido respecto a 2010 un 19,8% hasta los 10.917 Millones de euros, 2,4 puntos más que entre 2009 y 2010[29].

[28] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), *Estudio sobre Comercio Electrónico B2C 2011 (Octubre 2011).* [En línea] disponible en Internet: http://www.ontsi.red.es/ontsi/es/indicador/volumen-de-ventas-por-modelo-de-negocio-de-comercio-electr%C3%B3nico-b2c (última consulta 13 de julio de 2012).

[29] Estos son los datos actualizado en noviembre de 2012, por ONTSI.

C. El comercio electrónico entre empresa-administración pública B2A

Abarca los diversos tipos de servicio que ofrece la Administración Pública a las empresas para que éstas últimas puedan realizar trámites administrativos por vía electrónica[30]. En el siguiente apartado nos referimos a este supuesto pero en la modalidad de relación electrónica de la administración con todos los ciudadanos.

D. El comercio electrónico entre consumidor-gobierno C2A

Se trata de una relación en la que la Administración proporciona a los ciudadanos informaciones para que puedan realizar los trámites administrativos a través de Internet. En este sentido, cabe señalar que en el ordenamiento jurídico español existe una normativa jurídica que regula dicha relación.

El art. 1 de la Ley 11/2007, de 22 de junio, de "acceso electrónico de los ciudadanos a los Servicios Públicos(LAECSP)" «reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica»[31].

[30] España: Ley 11/ 2007.
Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en *BOE* núm. 150, 23 junio 2007; GÓMEZ VIETES, Á; y VELOSO ESPIÑEIRA, M.: *Economía digital*…op., cit., p. 86; vid. RICO CARRILLO, M*. Comercio electrónico…*op., cit., p.42; MODESTO ESPINAR, E. *El comercio…*op., cit., p. 35.

[31] Vid. Ley 11/2007, de…op., cit.,

Los objetivos que persigue la mencionada Ley de acceso electrónico de los ciudadanos a los Servicios Públicos son los siguientes: «

- Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso.

- Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

- Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general».

Sobre esta modalidad de comercio electrónico (A2C), existe un proyecto (Plan estratégico de sistemas de información de la Administración Pública) para su implantación en Guinea-Bissau, en el que se habla de un gobierno electrónico que tiene como objetivo acercar la Administración Pública a los ciudadanos mediante el uso de las nuevas tecnologías de la información y la comunicación. Por otra parte, se plantea en el proyecto que en esta era de la información, el gobierno electrónico es el instrumento más adecuado para poner los servicios públicos al alcance de los ciudadanos en cualquier momento y lugar, para la prestación de servicios más eficaces, eficientes y menos costosos; al tiempo que reduce la burocracia y la corrupción.

El Gobierno reconoce la necesidad de crear disposiciones jurídicas en materia de verificación de firmas digitales, sistemas de autenticación de terceros y pruebas electrónicas. Al mismo tiempo, señala que es necesario un marco jurídico autorizado por el Gobierno que facilite la difusión de la información, al tiempo que proteja la privacidad y los intereses de los ciudadanos y las empresas.

E. Comercio electrónico entre consumidores C2C

Se refiere a las transacciones comerciales privadas entre uno o varios consumidores que pueden tener lugar mediante el intercambio de correos electrónicos o el uso de tecnologías P2P (Peer to Peer), o en general en entornos cerrados de negocios como Ebay.

Tras analizar las distintas modalidades del comercio electrónico existentes en la actualidad, cabe concluir que el comercio electrónico indirecto no suscita mucha diferencia con el comercio tradicional; de hecho, existe semejanza ya que los bienes deben ser entregados físicamente. Esto trae aparejado que en dicha entrega también se aporte la documentación respectiva que acredite su venta, pudiéndose confirmar así la venta y el nacimiento de la obligación de pago. Sin embargo, el inconveniente se suscita con el comercio electrónico directo ya que su carácter "Virtual" dificulta la creación de mecanismos confiables de control fiscal y es más dificultoso debido a que las fronteras no existen en Internet.

Finalmente, intuyo que tras un periodo de comercio electrónico directo se pasará al comercio electrónico indirecto; o sea, mi hipótesis es que, si hubiese medios electrónicos de pago bien desarrollados en Guinea-Bissau, se impulsaría con naturalidad el comercio electrónico indirecto y a la vez el comercio electrónico directo en la medida en que el tipo de bien o servicio permita o no la ejecución de la entrega o la prestación por vía electrónica.

Hemos de reiterar que el comercio electrónico se ha convertido en un aspecto clave para la realización de negocios a nivel interno y mundial. Por lo que es necesaria una adaptación tanto del Estado de Guinea-Bissau como de las empresas guineanas que quieran seguir creciendo. Por lo que considero que el legislador guineano debe crear nuevas legislaciones más acordes con las nuevas tecnologías como detallamos en el último capítulo.

Así, para el desarrollo del comercio electrónico entre empresario y consumidor (B2C) en Guinea-Bissau, el legislador debe tomar en consideración la redacción de disposiciones que consagren y reconozcan jurídicamente dicha modalidad. Por ejemplo, adelantando aspectos que se retoman en el capítulo final.

- La Ley de servicios de la sociedad de la información y comercio electrónico, debe regular el régimen del establecimiento de los prestadores de servicios, el de las comunicaciones comerciales, el de la contratación por vía electrónica, el de la responsabilidad de los prestadores de servicios, incluidos los intermediarios, y el de los consumidores. Además, cabe subrayar la necesidad de definir en la futura Ley de servicios de la sociedad de la información y comercio electrónico, la figura de empresario o prestador de servicios de la sociedad de la información y comercio electrónico, así como la del consumidor o usuario.

- Ley de servicios de pago que incluya la protección de los consumidores y usuarios guineanos ante los problemas que puedan derivar del uso de medios de pago distintos del efectivo.

- Ley sobre servicios de la sociedad de la información y comercio electrónico.

- Ley de firma electrónica.

1.2. Concepto de pago electrónico

Para hablar de pago por medios electrónicos, en primer lugar, es necesario definir de forma muy breve qué es el pago en sentido general.

El pago es la contraprestación a la que se ha comprometido la parte contratante a cambio de una prestación que puede consistir en la entrega de un bien o en la prestación de un servicio. Según prevé el art. 1157 del Código Civil español, "no se entenderá pagada una deuda sino cuando completamente se hubiese entregado la cosa o hecho la prestación en que la obligación consistía"[32]. Se ha de definir el pago como un modo de extinción de las obligaciones que las partes han adquirido que supone el cumplimiento concreto de la prestación, ya sea a través de la entrega de una cantidad de dinero o de alguna cosa que represente el valor de la prestación de un servicio[33].

Una vez definido el pago en sentido general, es preciso definir en qué consiste el pago electrónico.

Según el art. 1 de la Recomendación 87/589/CEE de la Comisión, de 8 de diciembre de 1987, sobre un Código Europeo de Buena Conducta, el

[32] España: Real Decreto de 24 de julio de 1889, por el que se publica el Código civil, *BOE,* núm. 206 de 25 de julio de 1889.
p. 370; vid. PLAZA PENADÉS, J. "Contratación electrónica…"*op., cit.,* p. 451; vid. TRIAS DE BES, Xavier Añoveros. «El pago electrónico», *en* RICCIUTO, Vicenzo (coord*.). Il contratto telemático e i pagamenti elettronici. L`esperienza italiana e spagnola a confronto*. Milano: Etitore Dott. A. Giuffre, 2004, pp. 55 y ss; FRAMIÑAN SANTAS, Javier. «Pagos en la red. Medios de pago on line a través de Internet». en GÓMEZ SEGADE, José Antonio (dir.). *Comercio electrónico en Internet.* Madrid: Marcial Pons, 2001, pp. 373 y ss; DIEZ-PICAZO, Luís y GULLÓN, Antonio. *Sistema de derecho civil,* vol. II, 6.ª ed. Madrid: Tecnos, 1993, pp.178 y ss.

[33] GUIMARÃES, María. Raquel. "El pago mediante tarjetas de crédito en el comercio electrónico. Algunos problemas relativos a su naturaleza jurídica, marco contractual y régimen aplicable, desde una perspectiva comparada en los derechos portugués, español y comunitario", en M. MATA Y MARTIN, Ricardo (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, p. 169; vid. PLAZA PENADÉS, J. "Contratación electrónica…"*op., cit.,* p. 451; Según se establece en el art. 1.156 de CC, el pago es una de las causas de la extinción de las obligaciones contraídas. *Código*… op., cit., p. 370.

pago electrónico se define como «todas aquellas operaciones de pago efectuado con una tarjeta de pista magnética o con un microprocesador incorporado, en un equipo Terminal de Pago Electrónico (TPE) o Terminal de Punto de Venta (TPV)»[34].

Así pues, el pago electrónico[35] es el cumplimiento de la obligación de pago por medios electrónicos.

Por último, se ha de subrayar que el pago a través de medios electrónicos no necesariamente se realiza en el marco de un contrato electrónico[36] ya que "no existe una regla que exija pago manual en contrato manual ni pago electrónico en contrato electrónico"[37]. Es decir, como hacen

[34] COMISIÓN EUROPEA (1987): Recomendación de la Comisión, de 8 de diciembre de 1987, «relativa a un código europeo de conducta referente a los pagos electrónicos», (87/598/CE), *[Diario Oficial* núm. L 365 de 24/12/1987, 0072-0076]. También se pueden encontrar [En Línea] disponible en Internet: http://www.europa.eu/scadplus/leg/es/lvb/124018ª.htm. (última consulta 20 de julio de 2011); vid. DAVARA RODRÍGUEZ, M.: *Manual de Derecho Informático*. Navarra: Aranzadi, SA., 2004, p. 295; vid. ALONSO SOTO, R.: "Tarjeta de crédito, medios de pago electrónico y derecho de la competencia"*, en Estudio de Derecho Bancario Bursátil Homenaje a Evelio Verdera y Tuells*, t II. Madrid: La Ley, 1994, p.18.

[35] Siguiendo la tesis sostenida por la Profesora RODRÍGUEZ DE LAS HERAS BALLELL quien sostiene, que "hablar de pago electrónico significa tan sólo que se ha empleado un instrumento de pago capaz de cumplir su función socioeconómica gestionando la información en soporte digital y canalizándola mediante dispositivos electrónicos", RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo y la atribución de responsabilidad en el uso de tarjeta en la contratación electrónica", en RICO CARRILLO, M. (coord.) *Derecho de las Nuevas Tecnología.* Buenos Aires: La Roca, 2007, p. 322; VICENTE BLANCO, D. Javier. "Medios electrónico de pago y jurisprudencia competente en supuestos de Contratos Transfronterizos en Europa (Los criterios de competencia judicial del derecho comunitario europeo y su aplicación a las relaciones contractuales involucradas en los medios electrónicos de pago)", en MATA Y MARTÍN, R (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, pp. 270 y ss; TRIAS DE BES, X. A. «El pago…»*op., cit*., p. 56; Según sostiene IBAÑEZ, el pago electrónico "constituye, en la práctica, la transferencia de una información digital (trasladando la anotación contable de una cuenta a otra), que es autenticada, singularizada y firmada electrónicamente", en IBAÑEZ, J., *El control de internet.* Madrid: La catarata, 2005, p.78; por su parte VICENTE BLANCO, se puede definir los pagos electrónicos "como la realización de pagos a través de medios electrónico", VICENTE BLANCO, D J.: "Medios electrónico de…"*op. cit.,* p. 272.

[36] VICENTE BLANCO, D.: "Medios electrónico de…"*op. cit.,* p. 276.

[37] ILLESCAS ORTIZ, R. *Derecho de la contratación electrónica*. Madrid: Civitas, 2001, p. 344; sobre este mismo criterio, MADRID PARRA, sostiene que "aún cuando un contrato se haya celebrado por medios electrónicos, a la hora de su consumación, el cumplimiento de la obligación del pago se puede llevar a cabo por medios tradicionales o por los más modernos

notar algunos autores, y es evidente en la práctica, puede que un contrato de compraventa de un bien celebrado on line se pague físicamente contra reembolso al momento de la recepción de la mercancía, o puede que un contrato material se abone a través de un medio electrónico de pago, e incluso a través de Internet[38].

En este sentido, resumirá algún autor[39] que "puede darse con frecuencia que en una operación manual el pago se efectúe por vía electrónica aún cuando no será la más frecuente. Frecuente, por el contrario, es que en una operación de C-E el pago se lleve a cabo por vía electrónica aún cuando la contrapartida —hacer, no hacer o entregar—se lleve a cabo mediante medios materiales y físicos…" Y a continuación sostiene este mismo autor, que "existen puras operaciones contractuales de C-E en las que el cumplimiento de las obligaciones por ambas partes se lleva a cabo por

que facilitan las nuevas tecnologías", MADRID PARRA, Agustín. "Seguridad en el comercio electrónico", en ORDUÑA MORENO, Francisco J. (dir.*). Contratación y comercio electrónico*. Valencia: Tirant Lo Blanch, 2003, p.144; Según sostiene el profesor DAVARA RODRÍGUEZ, la contratación electrónica, es como "aquella que se realiza mediante la utilización de algún elemento electrónico cuando este tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo", en DAVARA RODRÍGUEZ, Ángel**.** *Manual de Derecho Informático*". Pamplona: Aranzadi, 1997, p. 171; por su parte, BARRIUSO RUIZ, la define como "aquella que con independencia de cuál sea su objeto, que puede ser también la informática, aunque no necesariamente, se realiza a través de medios electrónicos, que no tienen que ser siempre ordenadores", en BARRIUSO RUIZ, C. *La contratación electrónica*" Madrid: Dykinson, 1998, p. 359. según se prevé en el anexo h) de la Ley 34/2003, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, se entiende por "Contrato celebrado por vía electrónica o contrato electrónico: todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones" (*B.O.E*., núm. 166, de 12 de julio de 2002); en contra de esta tesis PARDO GATO, José Ricardo. *Las páginas web como soporte de condiciones generales contractuales*. Navarra: Aranzadi, S.A., 2003, p. 53; en cambio, siguiendo la tesis sostenida por PERALES VISCASILLAS quien sostiene que el contrato electrónico, se trata de los "contratos celebrados sin la presencia simultánea de comprador y vendedor, transmitiéndose la propuesta de contratación del vendedor y la aceptación del comprador, por medios telemáticos; por tanto, mediante el uso de ordenadores a través de una red telemática, que son sistemas de información gestionados por terceros distintos del oferente y del aceptante...", PERALES VISCASILLAS, María Del Pilar. "Formación del contrato electrónico", en *Régimen Jurídico de Internet*. CREMADES, J.; FERNÁNDEZ-ORDÓÑEZ, M.A.; e ILLESCAS ORTIZ, Rafael. (coords.). Madrid: La Ley, 2002, pp. 408-409.

[38] VICENTE BLANCO, D J.: "Medios electrónico de…"*op. cit.,* p. 276.

[39] ILLESCAS ORTIZ, R. *Derecho de…*op., cit., p. 344.

medios electrónico la muy difundida venta y entrega *on line* de un bien inmaterial (música o programas de ordenador) con pago electrónico de su precio por el comprador".

Una vez que hemos estudiado en los epígrafes anteriores en qué consiste el comercio electrónico, cuáles son sus modalidades, en qué se diferencian cada una de ellas, así como el pago electrónico, debemos pasar a analizar los medios que nos permiten efectuar dicho pago.

1.3. Concepto de medios de pago electrónicos

En los últimos años se ha demostrado que el progreso de las nuevas tecnologías de la comunicación y la transmisión de datos ha dado lugar al nacimiento y desarrollo del comercio electrónico[40], que impulsó a su vez el surgimiento de nuevos medios de pago ya que algunos medios tradicionales presentan inconvenientes o riesgos a la hora de pagar las compras efectuadas a través de Internet.

Uno de los elementos fundamentales del comercio electrónico, en la fase de cumplimiento de la obligación de pago, es el pago de los servicios prestados *"on line"* u "*off line*"[41]. Por esta razón, los medios electrónicos de pago están llamados a desempeñar funciones primordiales en las transacciones realizadas a través de una red abierta como Internet[42].

No obstante lo anterior, lo cierto es que el pago de los servicios prestados *on line* plantea algunos riesgos que los consumidores y usuarios han de afrontar en la utilización de los medios electrónicos de pago, como,

[40] MARTÍNEZ NADAL, A. *El dinero electrónico. Aproximación Jurídica*. Madrid: Civitas S.L., 2003, p. 17.

[41] LAFUENTE SÁNCHEZ, Raúl. *Los servicios financieros bancarios electrónicos*. Valencia: Tiran lo Blanch, 2005, p. 214; MARTÍNEZ NADAL, A., «Medios de pago en el comercio electrónicos», en *Actualidad Informática Aranzadi (AIA)*, núm. 37, octubre de 2000, pp. 5-11.

[42] GARCÍA MÁS, Francisco J. *Comercio y firma electrónicos. Análisis jurídico de los servicios de la sociedad de la información.* Valladolid: Edit. Lex Nova, 2001, p. 197.

por ejemplo, el uso fraudulento de estos medios, la sustracción o suplantación de datos personales y bancarios, lo que conlleva que la utilización de los medios de pago electrónicos no fuera inicialmente tan positiva como se esperaba[43].

En este sentido, coincidimos con el criterio de quienes sostienen que para dar respuesta a lo antedicho es necesario que los sujetos intervinientes en el proceso alcancen un modelo que garantice la seguridad y el buen funcionamiento de los sistemas de pago electrónicos[44].

En la actualidad existen medios de pago electrónicos, aceptados en varias tiendas virtuales y sitios de Internet, medios que agilizan las transacciones y procuran brindar la seguridad necesaria para llevar adelante el comercio electrónico.

Por su propia definición, los medios electrónicos de pago son mecanismos para efectuar la contraprestación consistente en el pago a través de Internet, ya que no es posible que el dinero en efectivo circule por la red; por ello se utilizan sistemas seguros que permitan al obligado a la

[43] COMISIÓN EUROPEA(1986): Comunicación de la Comisión Europea al consejo, y al Parlamento, «*una nueva baza para Europa: las tarjetas de pago electrónicas»,* 12 de enero de 1987, COM (86) 754 final; en la doctrina, MARTÍNEZ NADAL, señala que "el titular de una tarjeta de pago se muestra, en muchos casos reticente a enviar su número de identificación de tarjeta por la red para que le sea cargado, el precio de una compra por diversas razones: ya que el uso abierto de la Internet en la que puede ser interceptado por terceros(intercepción que puede ocurrir no solo en tránsito sino también en destino, una vez que los datos de la tarjetas están en manos del vendedor), la falta de conocimiento directo, por parte del comprador, del comerciante(en cuyas manos se pone una información sensible, lo cual puede dar lugar a usos fraudulentos, intencionados, dolosos directamente por parte del vendedor, o por negligencia en la custodia que permite el acceso no autorizado por parte de terceros)" en MARTÍNEZ NADAL, A. *El dinero electrónico*…op., cit., pp.18 y ss; vid. MARTÍNEZ GONZÁLEZ, M. "Mecanismo de seguridad en el pago electrónico". en MATA y MARTIN, Ricardo M (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, pp. 6 y ss.

[44] LAFUENTE SÁNCHEZ, R. *Los servicios financieros…*op., cit., p. 214.

contraprestación cumplirla cabalmente y al vendedor recibir el dinero por la prestación realizada, sea cual fuere la prestación[45].

En el Derecho comunitario, el art. 2, a) de la Recomendación de la Comisión 97/489/CE, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisor y titulares de tales instrumentos[46], establece que se entenderá por «"instrumento electrónico de pago", un instrumento que permita a su titular efectuar transacciones como las especificadas en el apartado 1 del artículo 1. Quedan incluidos en esta definición los instrumentos de pago de acceso a distancia y los instrumentos de dinero electrónico».

En el apartado 23 del art. 2 de la Ley 16/2007, de 13 de noviembre, de Servicios de Pago, que transpone al ordenamiento interno la Directiva

[45] Según sostiene BERNAL JURADO, en la "bibliografía existente sobre sistema de pago se utilizan frecuente los términos «medio de pago» e «instrumento de pago» de manera indistinta, situación que puede conducir a la confusión. Y que el «medio de pago» es todo aquello que tenga poder liberatorio de obligaciones, como es el caso de dinero de curso legal y del dinero bancario. Por el «instrumentos de pago» son aquellos mecanismos mediante los cuales se inicia la transferencia de dichos medios de pago entre las partes intervinientes en una transacción. En el caso de pago con efectivo, ambos conceptos coinciden por cuanto la entrega de moneda o billete tiene por sí misma poder liberatorio de deudas. Mientras que, el pago sin efectivo, el medio de pago transmitido es el dinero bancario y los mecanismos utilizado para ellos (tarjetas, cheques, transferencia, etc…)", en BERNAL JURADO, E. *El mercado español…*op., cit., p. 48, nota 1; en este mismo sentido BARUTEL MANAUT señala que "se tiende a confundir terminológicamente "medios de pago" con "instrumento de pago", y que los medios de pagos pueden ser clasificado en dos categorías: a) la moneda fiduciaria que comprende los billetes divisionarias; y b) la moneda espiritual, es decir los hechos materializados por anotaciones escritas, como el caso de las cuentas a la vista bancarias. La moneda fiduciaria o dinero en efectivo es un medio de pago que circula por sí solo. Mientras que los medios de pago espiritual necesitan instrumentos de pago que la hagan circular, ejemplo las tarjetas de pago", en BARUTEL MANAUT, Carles. *Las tarjetas de pago y crédito,* Barcelona: BOSCH, 1997, p. 17, nota 1; DAVARA RODRÍGUEZ, M. *Manual de...*op., cit., p. 295; por otra parte, según los autores LÓPEZ PASCUAL y SEBASTIÁN GONZÁLEZ, quienes definen el medio de pago como "un instrumento aceptado generalmente por los agentes intervinientes en una transacción para realizar el pago de bienes o servicios", en LÓPEZ PASCUAL, Joaquín y SEBASTIÁN GONZÁLEZ, Altina. *Gestión bancaria. Factores claves en un entorno competitivo,* 3. ª ed. Madrid: McGRAW-HILL/Interamericana de España, S.A.U., 2008, p. 312.

[46] UNIÓN EUROPEA: La Recomendación 97/489/CE, publicada en *Diario Oficial nº* L 208/50, de 02/08/1997, pp. 0052-0058.

2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, de servicios de pago en el mercado interior, se define el «Instrumento de pago» como "cualquier mecanismo o mecanismos personalizados, o conjunto de procedimientos acordados por el proveedor de servicios de pago y el usuario del servicio de pago, utilizado por éste para iniciar una orden de pago"[47].

A continuación dedicamos el apartado siguiente al estudio de las modalidades de los medios de pago en el comercio electrónico a través de Internet.

1.4. Las modalidades de medios de pago en el comercio electrónico

El gran avance de los servicios de la sociedad de la información y comercio electrónico[48] trae como consecuencia el desarrollo de nuevas modalidades de medios electrónicos de pago, incluyendo la expansión de los tradicionales medios de pago ya conocidos. Así pues, las modalidades de medios de pago utilizadas en el comercio electrónico se pueden clasificar en dos grupos:

[47] Según se define en el art. 1 de la Decisión Marco del Consejo de 28 de mayo de 2001 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo «instrumento de pago»: "todo instrumento material, exceptuada la moneda de curso legal (es decir los billetes de banco y las monedas metálicas), que por su naturaleza específica permita, por sí solo o junto con otro instrumento (de pago), al titular o usuario transferir dinero o un valor monetario --como, por ejemplo, tarjetas de crédito, tarjetas eurocheque, otras tarjetas emitidas por entidades financieras, cheques de viaje, eurocheques, otros cheques o letras de cambio-- que esté protegido contra las imitaciones o la utilización fraudulenta, por ejemplo, a través del diseño, un código o una firma". (2001/413/JAI).

[48] Según se establece en el inciso a) del anexo de la Ley 34 /2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE): Son servicios de la sociedad de la información: la contratación de bienes y servicios por vía electrónica, el suministro de información por vía electrónica, las actividades de intermediación, tales como: la provisión de acceso a la red, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de información, servicios o aplicaciones facilitadas por otros o la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet.

A. *Los medios de pago tradicionales*.

En este grupo de medios de pago tradicionales[49] podemos encontrar los que no funcionaban por medios electrónicos, como, por ejemplo, dinero efectivo[50], contra-reembolso, cheque, letra de cambio, pagaré, giro postal. Además, los que ya funcionaban por medios electrónicos, como es el caso de la tarjeta de crédito o débito y la transferencia bancaria.

B. Los medios de pago electrónicos.

Dentro de esta categoría de medios de pago electrónicos se encuentran aquellos medios de pago creados especialmente para el comercio electrónico que pueden ser clasificados de la siguiente forma: el cheque electrónico, la transferencia electrónica de fondos, las tarjetas monederos, medios de pagos a través de dispositivo móvil (*infra Cap.V, epígrafe 5.4*) y el dinero electrónico.

A continuación definiremos en qué consiste cada uno de ellos

1.4.1. Tarjeta bancaria (crédito o débito)

Las tarjetas de crédito o débito vienen siendo los medios de pago más utilizados en Internet[51]. Son instrumentos que permiten al comprador realizar compras en las tiendas virtuales, nacionales o internacionales, pagando las partes en sus respectivas monedas nacionales[52] y, a su vez, permiten al

[49] Vid. MADRID PARRA, A. "Seguridad en el…"*op., cit*., p. 145.
[50] Vid. DE MIGUEL ASENSIO, P. A. *Derecho...*op., cit., p. 431.
[51] Según pone de manifiesto ILLESCAS ORTIZ, "el pago mediante la tarjeta, que históricamente se inicia como una operación de comercio manual y que aún continúa siéndolo en un número largo de países entre muy numerosos operadores, se ha convertido desde hace lustros en medio electrónico generalizado…", en ILLESCAS ORTIZ R. *Derecho de la…op., cit.,* p. 341.
[52] Véanse SEOANE BALADO, Eloy. *La nueva era del comercio: el comercio electrónico los TIC al servicio de la gestión empresarial*. Vigo (España): Ideas Propias, 2005, p. 215; TRIAS DE BES, X. A. *El pago…op., cit*., pp.56 y ss; MARTÍNEZ NADAL, A.: «Medios de pago en el comercio electrónico», en *Actualidad Informática Aranzadi* (*AIA).* Octubre 2000, p. 6; existen una variedad de instrumentos electrónicos (tarjetas) que conforman el pago electrónico, por

vendedor el cobro de bienes o servicios prestados sin la intermediación del dinero en efectivo. Sin embargo, no escapan a los problemas de seguridad que abordaremos a lo largo de esta investigación[53].

Para que el proveedor de bienes o servicios pueda efectuar un cobro por Internet, es imprescindible contratar o instalar una pasarela de pago (Gateway) que le permita verificar los datos del comprador. A ello nos referiremos con más detalle (*infra Cap.II*)

1.4.2. Contra-reembolso

Es el único medio de pago utilizado en el comercio electrónico que implica uso de dinero metálico[54]. El pago de los productos se realiza off line, es decir, una vez que el vendedor u operador logístico procede a entregar la mercancía comprada[55] o, en su caso, a prestar el servicio. En este tipo de medio de pago intervienen tres sujetos: usuario, vendedor y operador logístico.

---

ej., las tarjetas de créditos, las tarjetas de débito, las tarjetas de compra, monederos electrónicos, tarjetas inteligentes, entre otras; también son considerados dentro esta expresión de pago electrónico, las tarjetas magnéticas, las tarjetas con chip, etc…; vid. MADRID PARRA, A. "Dinero electrónico: reflexiones sobre su calificación jurídica", en MADRID PARRA, A. (dir.). *Derecho del sistema financiero y tecnología.* Madrid: Marcial Pons, 2010, p. 40; vid., RAMOS HERRANZ, Isabel. "Tarjetas electrónica: problema de nuevo cuño y continuidad de los corte clásico", en VILLA GÓMEZ RODIL, Alfonso (dir.). *Contratos mercantiles especiales*. Madrid: Consejo General del Poder Judicial, 1997, pp. 419-495; MORENO NAVARRETE, M. A. *Derecho-e. Derecho del comercio electrónico.* Madrid: Marcial Pons, 2002, pp.125 y ss; GARCÍA SOLÉ, Fernando. "Aspectos sobre la incidencia de la tecnología en el mercado de tarjeta", en *Instituto Católico de Administración y Dirección de Empresas (ICADE),* núm. 43 enero-abril, 1998, pp. 80 y ss; BARUTEL MANAUT, C. *Las tarjetas de…op., cit.,* pp. 25 y ss; VEGA VEGA, José Antonio. *Contratos electrónicos y protección de los consumidores*. Madrid: Reus, S.A., 2005, p. 303.

[53] ESCOBAR ESPINAR, M. *El comercio electrónico. Perspectiva presente y futura en España.* Madrid: Retvisión, 1999, p. 131; LIBEROS, Eduardo (coord.). *El libro del comercio electrónico*. Madrid: ESIC Editorial, 2010, p. 306.

[54] SEOANE BALADO, E.: *La nueva era....*op., cit., pp. 212 y 213; el contra reembolso funciona de la siguiente manera, el cliente navega por website y elige los productos que desea adquirir. Cuando decide comprarlos, el sistema le requiere los datos personales, los cuales son remitidos a las oficinas de la empresa del proveedor junto con la información específica de la compra, la cual permitirá hacer la verificación previa al envío de los bienes. Cabe señalar que desde el punto de vista de seguridad del cliente el riesgo es mínimo por cuanto el pago se realiza cuando se entrega el bien.

[55] Vid. VEGA VEGA, J. A. "*Contratos electrónicos...*"op., cit*.,* pp. 348 y ss.

Se ha de concluir que este tipo de medio de pago presenta algunos inconvenientes, como por ejemplo: el retraso del pago y la necesidad de recoger físicamente el dinero en efectivo por parte de la persona que realiza la entrega.

1.4.3. Transferencia electrónica de fondos

La transferencia electrónica de fondos[56], se puede definir como el traspaso de fondos de una cuenta a otra que desempeña la función económica de efectuar pagos sin desplazamiento material de dinero[57]. Las transferencias electrónicas de fondos subyacen en una gran variedad de operaciones. Por ejemplo, las realizadas por tarjetas de crédito o débito, ya sean las simples retiradas de fondos en los cajeros automáticos, o una

[56] Para FERNÁNDEZ PÉREZ, "la transferencia de fondos es un método tradicional de pago que puede utilizarse al margen de Internet, ordenando una instrucción de pago a una entidad de crédito a favor de un tercero o comunicando los datos bancarios para que la otra realice el cargo. Pero, en la medida en que la transferencia sea usada mediante un instrumento de pago de acceso a distancia, como es las tarjetas de pago y los servicios de telebanco, puede ordenarse electrónicamente", en FERNÁNDEZ PÉREZ Nuria. *El nuevo régimen de la contratación a distancia con consumidores. Especial referencia a la relativa a servicios financieros*. Getafe (Madrid): La Ley, 2009, nota al pie n. 495, p. 335.

[57] Véanse, ALVARADO HERRERA, Lucía*. La transferencia bancaria.* Madrid: Consejo Económico y Social, 1999, pp. 25 y ss; MORENO NAVARRETE, *Derecho-e...*op., cit*.,* pp. 124-125; CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Mª. Asunción y RODRÍGUEZ DE CASTRO, Eduardo Pedro: *La contratación informática: el nuevo horizonte contractual,* 3.ª ed*.* Granada: Comares, 1999, p. 35; vid. HERNANDO, Isabel. *Contratos informáticos. Derecho Informático. Legislación y práctica.* San Sebastián: Librería Carmelo, 1995, pp. 475 y ss; MADRID PARRA, A.: "Dinero Electrónico: reflexiones sobre su calificación jurídica", en *Revista de Derecho Bancario y Bursátil (RDBB),* núm. 116, octubre-diciembre 2009, pp. 11 y ss; Siguiendo la tesis sostenida por el profesor ILLESCAS ORTIZ, quien señala que "el...carácter crucial que posee la transferencia electrónica de fondo respecto de los pagos electrónicos se basa en el hecho de que tales sistemas generalmente se basa en Mensajes de datos (MD) que el deudor dirige a su banco o tesorero en cuanto que el destinatario del mismo para que el banco o tesorería transfiera la cantidad de dinero debida a su acreedor o al banco o tesorero del mismo". Este mismo autor y por lo que se refiere al MD inicial este "contiene una declaración de voluntad de su emisor constitutiva de un orden de transferencia, general pero no necesariamente bancaria. Ese es el mecanismo jurídico de las tarjetas de crédito no manuales, de los monederos electrónicos, de los mecanismos electrónicos de pago activados por el ordenante—así los denominados cajeros automáticos- entre otros", en ILLESCAS ORTIZ R.: *Derecho de la…*, pp. 349 y ss., nota 403; ESCOBAR ESPINAR, M. *El comercio...op., cit.,* p. 131; VEGA VEGA, J. A. *Contratos electrónicos...op., cit.,* p. 304.

operación de pago en los terminales de puntos de venta (TPV) y muchas de las realizadas en Internet[58].

1.4.4. Cheque electrónico

El cheque electrónico[59] supone la migración del cheque de pap el al soporte electrónico, sustituyendo el talonario de cheques tradicional por una chequera electrónica de bolsillo[60]. El sistema de cheque electrónico se basa en la criptografía asimétrica (clave pública) y la firma electrónica[61], con la finalidad de garantizar la confidencialidad y la autenticidad.

[58] Sumándonos al criterio sostenido por el profesor ILLESCAS ORTIZ, tras señalar que "la transferencia electrónica de fondo y la compensación se encuentran presentes en todos los medios de pago que son objeto de oferta comercial en el mundo electrónico, de los cuales suelen ser componentes imprescindibles e incluso núcleo esencial", en ILLESCAS ORTIZ, R. *Derecho de la...op., cit.,* p. 345; este mismo autor ILLESCAS ORTIZ, R. *Derecho de la…o., cit.,* p.340; NOVAL PATO, Jorge. *Las transferencias bancarias indirectas. La actuación de bancos intermediarios y sistemas de pagos en la tramitación.* Granada: Comares, S.L., 2002, pp. 26 y ss, apunta que la transferencia electrónica de fondos no es más que "aquellas operaciones que han sido iniciada por medios electrónicos, en la que el cliente no ha tenido que recurrir a la cumplimentación de impresos o de cualquier otro tipo de documentos (cheque, pagaré,...)..."; vid. PASTOR SEMPERE, Mª. Del C. *Dinero*…op., cit., pp. 256 y ss.

[59] Vid. RAMOS HERRANZ, Isabel. «Cheques electrónicos», *Revista de Derecho Mercantil (RDM)*, núm. 229, julio-septiembre de 1998, pp. 1223-1249; RICO CARRILLO, M.: "El pago mediante…"*op., cit.,* p. 9; sostiene que un ejemplo de sistema de cheque electrónico es "e-Check" definido por el proyecto FSTC (Financial Service Technology Consortium), un consorcio conformado por varias entidades privadas o públicas, que colaboran de forma no competitiva en e l desarrollo de proyectos técnicos. El proyecto FSTC utiliza una tarjeta inteligente para implementar un " talonario de c heques electrónicos" seguro; LARA NAVARRA, Pablo y MARTÍNEZ USERO, José Ángel. *Comercio electrónico: la fidelización del usuario*. FUOC. Publicada: marzo de 2003 [En línea] Disponible en Internet: http://www.elprofesionaldelainformacion.com (última consulta, 6 de febrero de 2 012); DEVOTO, Mauricio**.** «La Economía Digital el dinero electrónico y el lavado de dinero». Revista de Derecho Informático (alfa redi), núm. 001, agosto del 1998, [En línea] Disponible en Internet: http:// www.alfa-redi.org/rdi-articulo.shtml?x=121 (última consulta, 26 de abril de 2012); vid. VEGA VEGA, J. A.: *Contratos electrónicos...*op., cit., pp. 335 y ss.

[60] BARRIUSO RUIZ, C. *Contratación…*op., cit., p. 462; PLAZA PENADEZ. J.: "Contratación*..."op., cit.,* p. 462.

[61] A juicio de VEGA VEGA, los métodos para transferir cheques electrónicos a través de internet no están tan desarrollados como otras formas de transferencias de fondos y, su funcionamiento en la red debe ir asociado a certificados y firmas digitales, en VEGA VEGA, J. A. *Contratos electrónicos...*op., cit., p. 304.

Incluye datos como fecha, nombre del beneficiario, cantidad y firma, entre otros. Se encuentran en un archivo electrónico seguro en el que el usuario define los datos relativos a la finalidad del cheque.

Este tipo de medio de pago electrónico puede utilizarse en casi todas las situaciones en las que se utiliza hoy en día un cheque impreso. También pueden utilizarse para autorizar los pagos a través de otros sistemas de pago que no estén basados en el cheque. Por ejemplo, un cheque electrónico puede ser utilizado para autorizar una transferencia electrónica de pago.

El funcionamiento de un cheque electrónico es similar al de un cheque de papel.[62] La chequera electrónica es un dispositivo electrónico que contiene herramientas de cifrado (público y privado), los certificados, los servicios públicos para desbloquear software y servicios públicos para llevar a cabo otras funciones. También puede contener instrucciones para mantener un registro seguro de las transacciones.

Este tipo de medio de pago en el comercio electrónico a través de Internet funciona de la siguiente forma: el usuario ingresa el número de ruta del banco y el número de su cuenta, así como su nombre, apellido, dirección y teléfono. Al instante se aprueba la transacción directamente en línea y el dinero es transferido a la cuenta del comerciante.

1.4.5. Monedero electrónico

Consiste en una tarjeta inteligente de prepago que contiene un microchip incorporado que se carga con una determinada cantidad de dinero

[62] Para el funcionamiento del cheque electrónico es imprescindible que el usuario tengan en su poder una chequera electrónica, que consiste en una tarjeta del tamaño de una tarjeta de crédito que puede contener datos y se inserta en un slot que puede ser incorporado en la mayoría de las computadoras portátiles que se ofrecen en el mercado. Además, puede ser otra tecnología (por ejemplo, almacenando los datos en otro soporte).

normalmente no muy elevada para efectuar pequeños pagos[63]. A medida que se van efectuando pagos se va reduciendo el importe hasta que se agota el saldo disponible pudiendo ser recargado o desechado[64]. Se creó para sustituir el uso de dinero en billetes y monedas de poco valor, pero su implantación ha sido muy limitada.

Cuando un usuario pretende hacer uso de este tipo de medio de pago, previamente debe disponer de un lector de tarjeta en su ordenador análogo

[63] Siguiendo el criterio sostenido por PLAZA PENADÉS, el monedero electrónico son "tarjetas de prepago que contienen un fondo de pago materializado en un chip que tienen incorporado, en el que se almacenan elementos o unidades de valor que previamente se han incorporado con cargo a la cuenta propia o mediante su cargo con efectivo, y siempre por un importe determinado que permite ir pagando hasta que dicho importe se agote, pudiendo ser recargable o desechable; con lo cual, y sus propias características, están diseñadas para pequeños pagos en efectivo", en PLAZA PENADÉS, J.: "Contratación..."*op., cit.,* p. 457; como pone de relieve la profesora RAMOS HERRANZ, "los problemas que plantea (...) las tarjetas-monedero son, de un lado, su escasa implantación y, de otro, la necesaria normalización de las mismas". Y señala la autora, que "por lo que se refiere a su implantación, el inconveniente principal es la ausencia de número suficiente de establecimientos comercial adheridos para que se implante su uso generalizado; sostiene la autora que dichas tarjetas implica una inversión por parte de pequeños comerciantes en los sistemas de lecturas de tarjetas monedero que en todo los casos sería rentable". Y sobre la normalización de la misma, la profesora señala que "es necesario la coordinación entre las diferentes entidades emisoras, con el fin de que todas las tarjetas sean compatibles en los distintos sistemas de lectura de los establecimientos comerciales y en los cajeros automáticos", RAMOS HERRANZ, I*. "Medios de pago electrónico"*, en BOTANA GARCÍA, Gema Alejandra (coord.). *Comercio electrónico y protección de los consumidores*, Madrid: La Ley, 2001, p. 547. BAUTECAS CALETRIO, Alfredo. *Pago con tarjeta de crédito. Naturaleza y régimen jurídico.* Navarra: Aranzadi, Monografía Asociada a la Revista Aranzadi de Derecho Patrimonial, núm. 15, 2005, p. 51; vid. MOLEJON ULLOA, Rusela. «Los medios de pago electrónicos. Limitaciones en su uso», *Revista de Derecho Informático: Alfa-redi*, núm. 101, diciembre de 2006, pp. 5-6. [En Línea], disponible en Internet. http://www.alfa-redi.org/rdi-articulo.shmt.(última consulta, 2 de enero de 2012); PASTOR SEMPERE, M. ª. *Dinero…*op, cit., p. 186; vid. FERNÁNDEZ PÉREZ, Nuria. *El nuevo régimen de la contratación a distancia con consumidores. Especial referencia a relativa a los servicios financieros*. Getafe (Madrid): La Ley, 2009, p. 341; vid. MARTÍNEZ NADAL, A. *Medios de pago…"op., cit.,* pp. 6 y ss; se ha de señalar que uno de los inconvenientes que presenta la tarjeta inteligente o monedero electrónico, sin lugar a duda, es la falta de estándares y, la incompatibilidad entre ellas; vid MARTÍNEZ NADAL, A.: «Medios de…*op., cit*., pp. 6 y ss.

[64] Vid. BERNAL JURADO, E.: *El mercado español de…op., cit.,* p. 57*;* BARRIUSO RUIZ, C. *Contratación…op., cit.,* p. 458; BROSETA PONT, M. y MARTÍNEZ SANZ, F. *Manual de...op., cit.,* p. 238; PLAZA PENADÉS, J.: "Contratación..."*op., cit.,* p. 457; RICO CARRILLO, M. «El pago mediante tarjeta en el comercio electrónico a través de Internet», *Revista de Comercio electrónico*, núm. 3, marzo de 2000, p. 4; CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Mª. A.; y RODRÍGUEZ DE CASTRO, E. P. *La contratación…op., cit.,* pp. 43 y ss.

a la disquetera. También para pagar las compras el cliente podrá cargar su tarjeta en el servidor web de su banco. Por lo que el ordenador del comprador o cliente se convierte en un cajero automático. Sin embargo, en el mercado existen nuevas modalidades de tarjeta de prepago que no precisan de dispositivo para poder efectuar un pago.

Por último, se ha de señalar que el uso del monedero electrónico como medio de pago no requiere de la intervención de la entidad bancaria como sucede con otros medios de pago en los que sí interviene la entidad emisora[65].

1.4.6. Dinero electrónico

El concepto de dinero electrónico es amplio y difícil de definir en un medio tan extenso como el de los medios de pago electrónicos (EPS). Al respecto existen diversas opiniones o criterios sostenidos por la doctrina que ha estudiado esta materia[66].

---

[65] Coincidiéndonos con la reflexión hecha por BAUTECAS, quien sostiene que las operaciones que se realiza a través del monedero electrónico "no existe la intermediación de la entidad bancaria, pero eso no quiere decir que las de entidades de créditos no desempeña ninguna otra actuación (por ejemplo las mayoría serán emitidos por ellas), sino que lo que no hacen es intermediar en la operación aprobándola o rechazándola, como sucede en las tarjetas de crédito", en BAUTECAS CALETRIO, A. *Pago con tarjeta...op., cit.,* p. 51, nota 35.

[66] MARTÍNEZ NADAL, A. *El dinero electrónico…op., cit.,* pp. 50 y ss; *Medios de pago…"op., cit.,* pp. 9-10; vid. MADRID PARRA, A.: «Seguridad en el…*op., cit*., pp. 148-151; a juicio de la profesora RICO CARRILLO, el dinero electrónico no es más que "un instrumento basado en el funcionamiento de una transferencia electrónica de fondo (TEF) que tiene por objeto facilitar el pago en operaciones generalmente concertadas a través de redes de comunicación pudiendo asumir distintas formas según la voluntad de las partes negociantes", en RICO CARRILLO, M.: *El pago mediante el dinero electrónico*. [En línea] disponible en Internet: http://www.ieid.org/congreso/ponencias/RicoCarrillo, Mariliana.pdf (última consulta, el 28 de abril de 2012); en este mismo sentido, RICO CARRILLO, M.: «Dinero electrónico», en *RCE,* núm. 31, octubre de 2002, pp. 5-6; por su parte, GUERRA BLAC, ha definido el dinero electrónico como «la representación por medio de un soporte informático de depósitos de dinero en curso legal u otros valores o activos financieros cuantificables, cuya circulación se realiza por medio de una transferencia electrónica de fondo», en GUERRA BLAC, Jaime Tomás. «La conclusión de contratos por medios informáticos», *Revista Informática y Derecho*, núm. 8, Mérida: Universidad Nacional de Educación a Distancia, Centro regional de Extremadura, 1995, pp. 63-131, en

Para algunos autores, el dinero electrónico es aquel "instrumento de pago reflejado en un soporte informático y que a través de la transferencias electrónicas de fondos persigue la misma finalidad que el dinero tradicional, dependiendo la efectividad del mismo de su realización"[67]. Para otros, el dinero electrónico es «un valor monetario cargado y almacenado en un soporte electrónico, normalmente una tarjeta inteligente o una memoria de ordenador»[68].

Sin embargo, siguiendo el criterio de otros autores, «el dinero electrónico, o moneda digital en efectivo es en esencia una información digital, autentificada, singularizada y firmada electrónicamente, que se admite como representación de éste y como un instrumento de pago»[69]. Tesis que compartimos por ser la más precisa o acertada que existe en la doctrina.

De acuerdo con el literal c) art. 2 de la Recomendación de la Comisión 97/489/CE, de 30 de julio de 1997, relativa a la transacciones efectuadas

---

especialmente p. 114; Véanse, MORENO NAVARRETE, M. A. *Derecho-e...op., cit.,* pp.123-124; PLAZA PENADÉS, J. "Contratación electrónica…"*op., cit.,* pp. 457-462; ibídem, «Impulso al empleo de técnicas electrónicas», en SÁNCHEZ CALERO, F. y SÁNCHEZ-CALERO GUILARTE, Juan (coords). *Comentario a la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero.* Elcano (Navarra): Aranzadi, 2003, pp. 803 y ss; ibídem "Dinero Electrónico: reflexiones...*op., cit.,* pp. 11 y ss; RAMOS HERRANZ, I. «Medios de pago…*op., cit.,* pp. 555 y ss; FRAMIÑAN SANTAS, Javier. "Pagos en la red…"*op., cit.* pp.386-396; vid., LÓPEZ PASCUAL, Joaquín; SEBASTIAN GONZÁLEZ, Altina. *Gestión bancaria. Factores claves en un entorno competitivo.* 3. ª ed. Madrid: McGraw-Hill/Interamericana de España, S.A.U, 2007, p. 321; vid. PATRONI VIZQUERRA, U. "El pago…"*op., cit*., p. 5; MOLEJON ULLOA, R. «Los medios de…*op., cit.,* pp.5-6; ECHEBARRÍA SÁENZ, Joseba Aitor. «El dinero electrónico: construcción del régimen jurídico emisor-portador», en MATA Y MARTIN, Ricardo M. (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, PP. 261 y ss; MATEO HERNÁNDEZ, José Luis. *El Dinero Electrónico en Internet. Aspectos técnicos y jurídicos.* Granada: Comares, 2005, pp. 380 y ss; VICENTE BLANCO, D J. «Medios electrónico de…op., cit., p. 279; BAUTECAS CALETRIO, A. *Pago con tarjeta...op., cit.,* pp. 53 y ss*;* MARTÍNEZ GONZÁLEZ, M. "Mecanismo de…*op., cit.,* p. 24.

[67]CARRASCOSA LÓPEZ, V; POZO ARRANZ, Mª. A y RODRÍGUEZ DE CASTRO, E. P. *La contratación…*op., cit., p. 34.

[68] DE MIGUEL ASENSIO, P.A., *Derecho privado de Internet* .Madrid: Civitas, 2002, pp. 436 y ss.

[69] BARRIUSO RUIZ, C. *Contratación…*op., cit., pp. 459 y ss.

mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisor y titulares de tales instrumentos[70], se define el instrumento de dinero electrónico como «un instrumento de pago recargable distinto de un instrumento de pago de acceso a distancia -ya sea una tarjeta en la que se almacenan electrónicamente los importes correspondientes o una memoria de ordenador- en el que se carga electrónicamente un valor, que permita a su titular efectuar transacciones como las especificadas en el apartado 1 del artículo 1 de la Recomendación»[71].

Por su parte, la Directiva 2000/46/CE, de 18 de septiembre, del Parlamento Europeo y del Consejo sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades(derogada), define el dinero electrónico en su inciso b) del apartado 3 del artículo 1 como «un valor monetario representado por un crédito exigible a su emisor: i) almacenado en un soporte electrónico; ii) emitido al recibir fondos de un importe cuyo valor no

[70] UNIÓN EUROPEA: La Recomendación 97/489/CE, de 30 de julio de 1997, relativas a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de tales instrumentos. Publicada en *Diario Oficial de las Comunidades Europeas (DOCE)* nº L 208/50, de 02/08/1997, pp. 0052-0058.

[71] El apartado primero del art.1 establece que la presente Recomendación se aplicará a las siguientes transacciones: «a) las transferencias de fondos, diferentes de las transferencias ordenadas y realizadas por entidades financieras, efectuadas mediante un instrumento electrónico de pago; b) la retirada de dinero en efectivo mediante un instrumento electrónico de pago y la carga (y descarga) de un instrumento de dinero electrónico en dispositivos como distribuidores automáticos de billetes y cajeros automáticos, así como en los locales del emisor o en una entidad con la que se haya suscrito un contrato para aceptar el instrumento de pago. 2. No obstante lo dispuesto en el apartado 1, para las transacciones efectuadas mediante un instrumento de dinero electrónico, no se aplicarán el apartado 1 del artículo 4, el segundo y el tercer guión de la letra b) del artículo 5, el artículo 6, las letras c), d) y el primer guión de la letra e) del apartado 2 del artículo 7, los apartados 1, 2 y 3 del artículo 8, y el apartado 2 del artículo 9. No obstante, cuando el instrumento de dinero electrónico sea utilizado para la carga (y descarga) mediante acceso remoto a la cuenta del cliente, la presente Recomendación se aplicará íntegramente. 3. La presente Recomendación no se aplicará a las siguientes transacciones: a) el pago mediante cheques; b) la función de garantía de determinadas tarjetas en relación con el pago mediante cheques».

será inferior al valor monetario emitido; y iii) aceptado como medio de pago por empresas distintas del emisor»[72].

Según establece el legislador comunitario en el considerando (3) de la Directiva 2000/46/CE, se considerará el dinero electrónico como un sustitutivo electrónico de las monedas y los billetes de banco, almacenado en un soporte electrónico como, por ejemplo, una tarjeta inteligente o la memoria de un ordenador y que, en general, está pensado para efectuar pagos electrónicos de cuantía limitada.

Sin embargo, el apartado 2 del art. 2 de la Directiva 2009/110/CE, del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE, define el dinero electrónico, como «todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico»[73].

Por su parte, la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero(LMRSF)[74], que regula el dinero electrónico

[72] UNIÓN EUROPEA: Directiva 2000/46/CE, del Parlamento Europeo y del Consejo de 18 de septiembre de 2000 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades. Publicado en *DOCE* nº. L 275, de 27 de octubre de 2000, p. 37.

[73] UNIÓN EUROPEA: Directiva 2009/110/CE, del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE, definí el dinero electrónico. Publicado en *DOUE,* L 267, 10 octubre de 2009.

[74] España: Ley sobre medidas de reforma de sistema financiero, 2002. Medida de Reforma de Sistema Financiero: Ley 44/2002, de 23 de noviembre, en el *BOE* núm. 281;

y que incorpora al ordenamiento español la Directiva 2000/46/CE, a la que hemos hecho referencia con anterioridad, en el apartado 2 del art. 21 establece que «se entenderá por dinero electrónico el valor monetario representado por un crédito exigible a su emisor: a) Almacenado en un soporte electrónico, b) Emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido, y c) Aceptado como medio de pago por empresas distintas del emisor».

En cambio, el legislador español establece en el apartado 2 art. 1 de la Ley 21/2011, de 26 de julio, de dinero electrónico, que transpone al ordenamiento jurídico español la Directiva 2009/110/CE, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión de dichas entidades, que «se entiende por dinero electrónico todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley

---

para MARTÍNEZ NADAL, "la definición que da el legislador español coincide, pues, prácticamente de forma literal con la definición comunitaria. Sin embargo, como aportación propia del legislador español, existe únicamente el último párrafo de este apartado segundo del art. 21, que prohíbe a los emisores la recepción de fondos por importe superior al valor monetario emitido. De manera que, por aplicación literal y conjunta de esta prohibición y del requisito del apartado b) (que establece que los fondos recibidos por la entidad emisora no será de valor inferior al valor monetario emitido) resultaría que en el derecho español no sólo está prohibida la emisión por debajo de la par (igual que en el derecho comunitario) sino también por encima de la par (sin prohibición expresa en la directiva comunitaria)".

Y a continuación, señalan que "la falta de mayor información sobre el origen de esta previsión, cabría quizá relacionarla con la característica de gratuidad e inexistencia de costes para el usuario que se considera que debería cumplir el dinero electrónico de forma similar al dinero en efectivo", en FERRER GOMILA, José Luis y MARTINEZ NADAL, A.: "Aproximación al Concepto Jurídico de Dinero Electrónico". Ponencia presentada en *el Segundo Congreso de Comercio Electrónico CSE '03*, celebrado Universitat de les Illes Balears, en junio de 2003, Barcelona. [En línea] Disponible en Internet*:* http:// www.criptored.upm.es/guiateoria/gt_m081e.htm - 4k (última consulta 12 de enero de 2012)*;* PASTOR SEMPERE, M.ª *Dinero…op., cit.,* p. 154. sostiene que el dinero electrónico no se puede ser considerado como un valor monetario almacenado en una tarjeta, sino que hay que definirla como "un titulo de crédito digital firmado por un banco o por una institución no bancaria, que contiene la promesa de pagar, a la vista, al portador y que puede ser transmitida a través de cualquier red telemática de flujo de bits".

16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico»[75].

Finalmente, cabe resaltar que tanto el legislador comunitario como el español introducen una nueva definición del dinero electrónico en la que se añaden nuevas expresiones como «*medios electrónicos o magnéticos*» que no estaban recogidas en l as anteriores normativas, la expresión que se utilizaba era "*almacenado en soporte electrónico*"[76].

A continuación, examinaremos algunos de l os sistemas de dinero electrónico existente en la actualidad.

1.4.6.1. *Análisis de los sistemas de dinero electrónico*

En la actualidad se usan diversos tipos de s istemas de dinero electrónico, entre los que cabe señalar:

A. Sistemas basados en un software (software-based)

En este sentido, se pueden definir como aquellos sistemas que funcionan a través de la instalación de un programa en el ordenador[77] y se pueden clasificar en efectos de su exposición en dos grupos:

a) Los pioneros en el mercado

Aquellos que son pioneros en el mercado: E-cash[78]y Millicente que se basan únicamente en programas de ordenador; y

[75] España: la Ley 21/2011, de 26 de julio, de dinero electrónico, que transpone al ordenamiento jurídico español la Directiva 2009/110/CE, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión de dichas entidades, en *BOE*, núm. 179, 27 de julio de 2011, 20 p;

[76] vid. ILLESCAS ORTIZ, R. «las nuevas responsabilidades electrónicas legales y su aseguramiento», en *II Congreso sobre las Nuevas Tecnologías y sus repercusiones en el seguro: Internet, Biotecnología y Nanotecnología.* Barcelona, *17 y 18 de noviembre de 2011.* Madrid: SEAIDA, 2012, pp. 21-23.

[77] Vid. DEVOTO, M. La economía digital el dinero electrónico y el lavado de dinero, en *Revista de Derecho Informático,* núm. 001, Agosto 1998. [En línea] disponible en Internet: http://www.alfa-redi.org/rdi-articulo.shtml?x=121 (última consulta, 20 de agos to de 2012); FRAMIÑAN SANTAS, J. "Medios de pago…"*op., cit.,* p. 386.

b) Los nuevos en el mercado: Ukash, Hal-cash, Paypa, Moneybooker, y Google Checkout

a1) E-cash

Desarrollado por la empresa holandesa Digicash, con sede en Amsterdam[79], fue el primer sistema de pago certificado y supone una parte importante de las transacciones realizadas actualmente con dinero electrónico a través de Internet. Utilizando el software de DigiCash, el cliente crea "tokens" en blanco y los envía a través de un sobre digital oculto al banco para su certificación.

El banco firma cada token, carga en la cuenta del cliente la cantidad de e-cash emitido y devuelve los tokens a través de Internet. Este tipo de sistema hace uso de la criptografía de clave simétrica y asimétrica con la finalidad de garantizar la seguridad en el sistema[80]. Para el uso de e-cash, las partes necesitan tener abierta una cuenta en uno de los bancos que emite el dinero electrónico[81], siendo la propia entidad bancaria la que facilita el software de emisión del dinero electrónico.

a 2) Millicent

Es un mecanismo de pago desarrollado por la empresa americana "Digital´S" (Systems Rescarchs Center, con sede en California), cuyo objetivo es promover un sistema para efectuar transacciones de pequeños

[78] Digicash fue fundada por David Chaum. http://www.digicash.nl (última consulta 12 de septiembre de 2012).

[79] Este sistema fue creada por David Chaum, un experto en la criptografía; vid. RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo…*op., cit.,* p. 327.

[80] MARTÍNEZ NADAL, A. *El dinero electrónico*…op., cit., p. 58; vid., http://www.ecash.net (última consulta 2 de diciembre de 2012); ITEANU, Olivier. *Internet et le Droit. Aspects juridiques du commerce électronique.* Paris: Éditions Eyrolles, 1996, p. 142.

[81] FRAMIÑAN SANTAS, Javier. "Pago en la Red. Medios de pago on line a través de Internet", en GÓMEZ SEGADE, José Antonio y ALBOR BALTAR, Ángel F.: *Comercio electrónico en Internet.* Madrid: Marcial Pons, 2001, p. 388; RICO CARRILLO, M.: *Comercio...op., cit.,* p. 174.

valores en Internet. Dicho sistema está basado en un modelo de apuntes que descansa en un agente (broker).

El broker es el intermediario que acepta los pagos de los consumidores y apunta el crédito a los comerciantes. Este tipo de sistema emite sus propios apuntes a los consumidores, eliminando la necesidad de relaciones previas entre cliente y vendedor antes de la transacción. El sistema Millicent trata de reducir costes, incrementar el volumen de intercambios y ofrecer ciertos niveles de seguridad a los vendedores[82]. Se realiza a través de la noción de "apunte digital específico del vendedor".

Una forma frecuente para su generación es el uso de una clave secreta para encriptar un número de serie. El valor encriptado y el índice de la clave forman el apunte. Cuando el apunte es recibido por el vendedor, es descodificado para verificar que contiene un índice válido que no ha sido utilizado anteriormente.

El apunte es como el dinero en efectivo pues posee valor intrínseco, pero, a diferencia de éste, ostenta dicho valor únicamente cuando se gasta con un comerciante específico.

- ✓ *Ventajas e inconvenientes*

Una de las ventajas que presenta el Millicent es que no existe un servidor central sino un conjunto de agentes que sólo se encuentran implicados en una parte de la transacción, con lo que se reducen los costes de comunicación; los costes criptográficos son menores y adecuados al monto de la operación; disminuyen los costes contables pues, en lugar de mantenerse cuentas separadas para cada combinación de cliente-vendedor,

[82] FRAMIÑAN SANTAS, J. "Medios de pago…"*op., cit.,* p. 394. Vid. BIDGODI, Hossein. *Electronic commer. Principles and practice.* San Diego (California): ACADEMIC PRESS, 2002, pp. 203 y ss.

cada cliente mantiene una sola cuenta con el agente y cada vendedor tiene cuentas de larga duración con unos pocos agentes.

Sin embargo, uno de los mayores problemas del sistema es la seguridad. Sus creadores asumen que puede darse cierto fraude, pero Millicent fue desarrollado como un mecanismo de pago para pequeñas cantidades[83]. Podría incorporar mecanismos más seguros de encriptación, pero entonces los costes inherentes excederían el valor de las transacciones para las que es válido.

b) Los nuevos modelos de dinero electrónico

b1) Ukash

Podemos comenzar diciendo que Ukash es una red global de dinero electrónico en la que se proporciona a los consumidores y usuarios una forma alternativa de pagar on line por la compra de bienes o el uso de servicios. Este sistema ha revolucionado la forma de comprar por Internet al convertir las monedas y los billetes en dinero electrónico en forma de vale.

Se ha de resaltar que cada vale es único y contiene un número de seguridad de 19 dígitos que se puede usar una sola vez. Una de las ventajas que posee el Ukash es que el cliente está menos expuesto al robo de identidad gracias a la existencia de más de 10.000 millones de combinaciones y al hecho de que no necesita proporcionar su nombre o dirección. Sin embargo, al igual que sucede con el dinero en efectivo, el riesgo de apropiación o uso no autorizado es posible.

Entre las medidas de prevención del uso fraudulento que debe adoptar el usuario de este tipo de sistema señalaremos:

- ✓ Hacer uso de Ukash únicamente en los sitios web seguros.

[83] FRAMIÑAN SANTAS, J. "Medios de pago…"*op., cit.,* p. 394; vid. RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo…"*op., cit*., p. 327.

- ✓ No facilitar el código de su vale Ukash a un tercero.

- ✓ No necesita facilitar los datos de su tarjeta de crédito o débito para usar Ukash.

- ✓ No debe r evelar ningún tipo de información personal para usar Ukash.

Para la adquisición de U kash, el cliente debe entregar dinero en efectivo en una tienda en la que vendan Ukash. A cambio, recibirá un vale por la cantidad entregada; y una v ez que el cliente tiene en su poder el número de vale puede proceder a utilizarlo en cualquiera de los sitios web que acepten dicho sistema de pago.

b2) Hal-Cash

Es un servicio bancario que permite enviar dinero a cualquier persona a su teléfono móvil y retirarlo de forma inmediata en un cajero sin ser cliente del banco ni usar tarjetas de crédito. Su funcionamiento es el siguiente: se da la orden de envío a través de una oficina, cajero automático, teléfono o Internet, al móvil seleccionado. Para ello habrá que indicar una clave secreta de cuatro dígitos. A continuación, es necesario hacerle saber esta clave secreta al beneficiario de la transferencia por cualquier medio de telecomunicación.

Por su parte, Hal Cash envía un SMS al móvil del beneficiario indicándole el importe del envío y una referencia de la operación. El beneficiario de la operación debe acudir a un cajero adherido a Hal Cash con la clave secreta, la referencia de la operación recibida a través del SMS y el número de móvil para retirar el efectivo.

b 3) Paypal

Es un sistema desarrollado por una empresa estadounidense, propiedad de eBay[84], perteneciente al sector del comercio electrónico por Internet que permite la transferencia de dinero entre usuarios que posean correo electrónico. PayPal[85] también procesa peticiones de pago en comercio electrónico y otros servicios webs, por los que cobra un porcentaje al vendedor. La mayor parte de su clientela proviene del sitio de subastas en línea eBay.

En los últimos años PayPal se ha convertido en un proveedor de servicios de pago muy popular entre los compradores on line.

Una de las ventajas que ofrece consiste en la facilidad para abrir una cuenta: se tarde unos cinco minutos y la información requerida es mínima. Ofrece la posibilidad de pagar con tarjeta de crédito, mediante transferencia o con saldo PayPal, y datos tales como el número de la cuenta corriente no son revelados al vendedor. Para los comerciantes se trata de una solución de pagos sencilla y poco costosa.

b 4) Skrill (Moneybookers)

Es un sistema de dinero electrónico que permite los pagos y transferencias de dinero a través de Internet. Sirve como una alternativa

[84] En octubre de 2002, EBay compró PayPal, cuando ya era el método de pago usado por más del 50% de los usuarios de eBay, y el servicio competía con el sistema propio de eBay, BillPoint.

[85] Fue fundado inicialmente bajo el nombre de Confinity en 1998 por Peter Thiel y Max Levchin. Luego de su fusión con X.com fue renombrado PayPal. Vale la pena destacar que todavía conservan el dominio x.com. Una de sus primeras sedes fue la *165 University Avenue* en Palo Alto, California, donde comenzaron varias empresas de Silicon Valley. En principio, PayPal era un servicio para transferencias de dinero vía PDAs. Pero el pago en la web se convirtió en un negocio más apetecible. Una agresiva campaña de marketing ofreciendo primero 10$ y luego 5$ por registrarse en el sistema, provocó que el crecimiento fuese meteórico: entre un 7 y un 10% al día entre enero y marzo de 2000; vid., SEOANE BALADO, E.: *La nueva era....*op., cit., pp. 220-221.

electrónica a los métodos tradicionales en papel como los cheques y giros postales. El sistema se basa en realizar o procesar los pagos para sitios web, sitios de subastas en línea, y otros usuarios corporativos.

Al igual que muchos competidores servicios de transferencia de fondos en línea (por ejemplo, *PayPal*), *Skrill (*Moneybookers)[86] requiere verificación de identidad antes de usar su servicio para minimizar el fraude y prevenir el blanqueo de dinero.

Skrill cuenta con una Cartera Digital, que es una de las más importantes del mundo y está firmemente asentada como una alternativa real frente a todos los métodos de pago tradicionales. Permite que cualquier cliente registrado pueda pagar en línea de forma cómoda y segura sin revelar datos financieros personales, así como enviar y recibir transferencias de dinero, simplemente con una dirección de correo electrónico.

B. Sistemas basados en hardware

a) Cybercash

Fue creada en 1994 por CyberCash Corporation[87]. Constituye un mecanismo de pago muy similar al protocolo SET que ofrece a los comerciantes una solución rápida y segura para procesar los pagos con tarjeta de crédito a través de Internet. El usuario necesita tener un software especial de cartera que resida permanentemente en su máquina, como en el caso de Microsoft Wallet, o bien que resida en el servidor de CyberCash.

También el comerciante necesita instalar un software en su servidor, que genera una comisión de la venta para CyberCash, que hace como tercera

[86] Fue creado el 17 de junio 2001, y se puso en marcha el 1 de abril de 2002. https://www.moneybookers.com/app/products.pl

[87] Véanse PATRONI VIZQUERRA, U. "El pago…"*op., cit*., p.5; MOLEJON ULLOA, Rusela. Los medios de pago electrónicos. Limitaciones en su uso. *Revista de Derecho Informático: Alfa-redi*, núm. 101, diciembre de 2006, pp. 5-6. [En Línea], disponible en Internet. http://www.alfa-redi.org/rdi-articulo.shmt.(última consulta el 2 de enero de 2012); vid. http://www.ecash.net (consultada el 2 de diciembre de 2012).

parte de confianza entre el comerciante y cliente[88]. De esta forma, el comerciante no necesita adquirir un s istema de back-office para el procesamiento de las operaciones de venta con tarjeta, puesto que es el servidor de CyberCash, el que gestiona con el banco todas las operaciones de pago.

Es tipo de sistema permite que los datos bancarios no sean conocidos por el comerciante, ya que éste sólo dispone de los datos de envío y de los productos de compra[89]; tampoco el servidor de CyberCash puede ver los datos de la compra[90]. De este modo, el sistema concede al usuario una mayor seguridad al permitir que su número de tarjeta nunca llegue a ser conocido por el comerciante sino solamente por el servidor de CyberCash y, por supuesto, por los bancos participantes.

Además, garantiza la seguridad al comerciante ya que el cobro de la mercancía se produce incluso antes de que sea vendida, como ocurre en las transacciones en los puntos de venta de las tiendas.

Por último, cabe señalar que el sistema CyberCash actúa como intermediario entre el comerciante y el usuario asegurando que el primero reciba el pago mientras que éste último recibe el producto de la compra. Tanto el software del cliente como del servidor son gratuitos y están disponibles para múltiples plataformas.

[88] ITEANU, Olivier. *Internet et le Droit. Aspects juridiques du commerce électronique.* Paris: Éditions Eyrolles, 1996, pp. 142-143.

[89] BARRIUSO RUIZ, C. *Contratación...op., cit.,*

[90] RAMOS SUARES, F.: "Aspectos a tener en cuenta para implantar una solución de comercio electrónico segura y efectiva (Tercera parte)". Publicada en noviembre 2001, y actualizada en el 5 de noviembre 2007 [En línea] disponible en Internet: http://www.masterdisseny.com/master-net/legalia/0015.php3 (última consulta 14 de agosto de 2012).

b) Mondex

Son tarjetas monedero creadas por el NatWest Bank como un sistema de pago off line y están totalmente basadas en el mecanismo de las tarjetas con chip, pero se están reorientando hacia Internet[91]. Los fondos en Mondex pueden ser transferidos de una tarjeta a otra sin necesidad de verificación por parte de un banco o cualquier otro procedimiento.

El sistema electrónico opera a través de una tarjeta inteligente que almacena información en un microchip. El chip contiene el valor de los fondos y el programa de seguridad que protege las transacciones de una tarjeta a otra. Esa información puede ser transferida a través de la línea telefónica o de Internet y el dinero electrónico puede ser bloqueado utilizando un código elegido por el usuario. Este tipo de sistema permite operaciones entre individuos de manera directa sin la intervención de bancos o terceros.

Al mismo tiempo proporciona la seguridad en dos aspectos fundamentales del sistema: "el hardware de la tarjeta" y "el proceso de transferencia". Cada tarjeta se encuentra certificada por una firma digital Mondex y el proceso de transferencia, no sólo verifican la autenticidad de la otra, sino que se trata de un proceso secuencial en el que los fondos son deducidos de la tarjeta del consumidor con anterioridad a su adscripción a la tarjeta del comerciante.

De hecho, el sistema Mondex presenta algunos inconvenientes como, por ejemplo, que el usuario cuente con lectores de tarjetas (lo que supone un coste adicional) y el que no quede claro cuál es la ganancia de los bancos

[91] RICO CARRILLO, M. Comercio...op., cit., p. 172, según sostiene esta autora el sistema Mondex fue concebido originalmente como sistema off-line para dinero en metálico basado en funcionamiento del monedero electrónico. Ante las ventas conseguido en Internet se ha ideado una variante de este sistema denominado Mondex on the Net cuyo objetivo principal consiste en la implantación del sistema Mondex para pagos on line a través de la Red;vid http://www.mondex.com, nota p. n. 244.

pues no es necesaria su intervención salvo para el depósito o el intercambio de la tarjeta por efectivo.

Como conclusión, podemos afirmar que las modalidades o sistemas de pago incluidas dentro del concepto de dinero electrónico están especialmente diseñadas para dar cumplimiento a las obligaciones pecuniarias contraídas en los contratos electrónicos, por lo que se adaptan al medio tecnológico y, al mismo tiempo, suponen ventajas en lo que se refiere a la seguridad y limitación del riesgo de pérdida. Sin embargo, dichos sistemas presentan inconvenientes que impiden su utilización masiva en Internet[92].

A raíz de esto, la tarjeta de pago (crédito) se ha convertido en el medio más utilizado en el comercio electrónico a través de Internet[93], sobre todo por su elevado nivel de popularidad entre consumidores y usuarios, a lo que hay que sumar su fácil utilización para ejecutar el pago a través de Internet.

No obstante lo anterior, lo cierto es que el uso de la tarjeta como medio de pago en Internet plantea algunos riesgos o inconvenientes, sobre todo en lo relacionado con la seguridad en las transacciones electrónicas. La falta de seguridad en las operaciones de pago realizadas mediante el uso del número de la tarjeta de crédito en Internet es uno de los mayores problemas al que se enfrentan los usuarios. La mayor parte de ellos temen enviar sus

[92] Vid. MARIMÓN DURÁ, Rafael. *La tutela del usuario en el contrato bancario electrónico.* Monografía asociada a Revista Aranzadi de Derecho y Nuevas Tecnologías, núm. 8. Cizur Menor (Navarra): Aranzadi, SA, 2010, p. 220, para este autor "dichos inconvenientes(…) tienen que ver con el hecho de que todavía no se haya podido instaurar un sistema generalmente aceptado y dotado de la suficiente liquidez o fungibilidad, como para poder actuar de una forma autónoma frente sistemas de pago tradicionales".

[93] La Asociación para la Investigación de Medios de Comunicación (AIMC) presentó en Madrid, el día 23 de febrero de 2011, los resultados de la 13ª encuesta a usuarios de Internet (Navegantes en la Red). Y siguiéndonos los resultados obtenidos por este mismo organismo, la tarjeta de crédito es el medio de pago más utilizada en la Red, "por el 75% de los usuarios. AMIC, es gestora de los más importantes estudios de audiencia en España, entre otros el EGM, ha presentado los resultados de la 14ª Encuesta a Usuarios de Internet (Navegantes en la Red). [En Línea] disponible en Internet: http://www.aimc.es.(última consulta 26 de noviembre de 2012).

datos personales y bancarios ya que corren el riesgo de ser interceptados durante la comunicación entre los servidores y que el producto comprado no llegue nunca a sus manos. Por su parte, el proveedor de bienes o servicios también teme que los datos de la tarjeta utilizada sean falsos.

Se ha de resaltar que entre los distintos medios de pago clasificados a lo largo de este capítulo, optaremos por estudiar las tarjetas de pago (crédito) como el medio más utilizado en el comercio electrónico, especialmente en Internet, y que más se sigue utilizando en la actualidad. Por lo tanto, hemos de subrayar que, a continuación, analizaremos las distintas definiciones que dan diversos autores y la doctrina sobre las tarjetas de pago, su clasificación, la diferencia existente entre tarjeta de crédito y débito, y, por último, se estudiarán los sujetos intervinientes en las operativas de pagos mediante tarjeta en el comercio electrónico.

Finalmente, al ser las tarjetas de crédito el medio de pago más utilizado en el comercio electrónico en los países desarrollados, como es el caso de España, hemos optado por estudiarlas a lo largo de este trabajo con el objetivo de proponer su implementación en Guinea-Bissau.

1.5. Tarjeta electrónica de pago y su clasificación

Antes de continuar con el estudio de la tarjeta como medio de pago electrónico en Internet, creemos necesario explicar la terminología que emplearemos a lo largo de esta investigación. Existen posturas doctrinales que aluden a la tarjeta de crédito como medio de pago electrónico, por ser éste el término más utilizado para referirse a las tarjetas en general. Para algunos es una tarjeta de pago o de plástico. De hecho, tanto la doctrina como la jurisprudencia utilizan la terminología “tarjeta de crédito” como denominación general y pretendidamente omnicomprensiva, criterio que no compartimos, ya la tarjeta de crédito es sólo una de las modalidades existentes en el sistema de tarjetas de pago electrónico, que cumple

funciones diferentes a los demás tipos de tarjeta, por ejemplo la tarjeta de débito, tarjeta de compra o monedero electrónico.

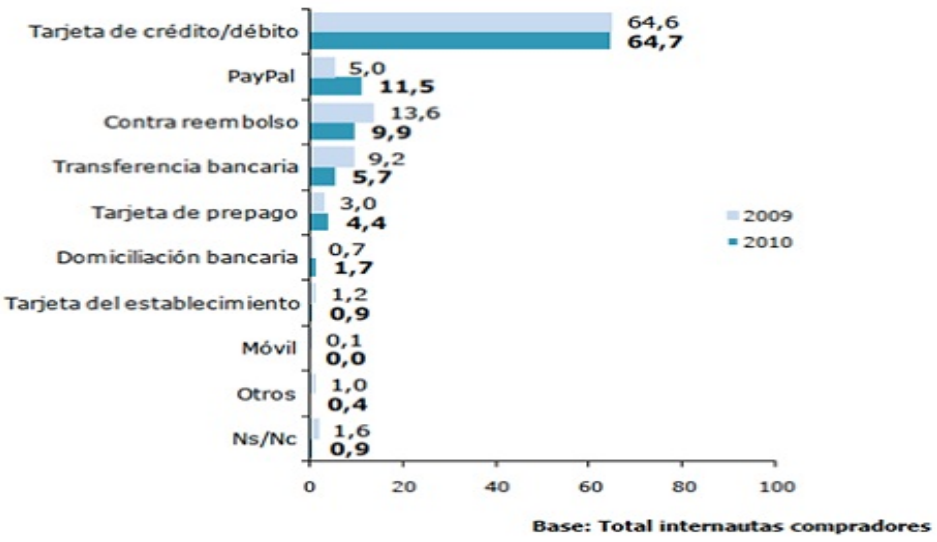
Siguiendo las disposiciones de la Comunidad Europea y alguna doctrina, creemos que lo más correcto es emplear a lo largo del trabajo la expresión "tarjeta electrónica", por ser la terminología más adecuada a nuestro estudio, ya que hoy en día todas las tarjetas llevan incorporados elementos electrónicos para funcionar en las redes de pago electrónico.

En la actualidad, la tarjeta electrónica, ya sea de crédito o de débito, constituye, por su aceptación, la principal categoría dentro del pago electrónico, convirtiéndose en un instrumento utilizado en operaciones de adquisición de bienes de consumo y de pago de servicios personales de bajo coste.

Según el informe del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de 2011, dos de cada tres compradores on-line (64,7%) prefieren pagar sus compras por Internet a través de tarjeta de crédito o débito. Esta preferencia se mantiene a lo largo de los últimos años[94]. Por otro lado, PayPal se convierte en el segundo medio de pago preferido para los compradores on-line (11, 5%). La tercera opción preferida por los consumidores es el pago contra reembolso (9,9%), mientras que las transferencias bancarias se sitúan en cuarto lugar (5,7%). Obsérvese el gráfico 2 en el que se reflejan los datos sobre dichas cuestiones.

[94] En este mismo sentido, según el informe del Observatorio Aragonés de la Sociedad de la Información (OASI), presentado en 2008, el 70,5% de los consumidores utilizaron la tarjeta de crédito para hacer sus compra en la red abierta como Internet; por tal razón, dicho medio de pago se convierte en el medio de pago más utilizado por los usuarios en la Internet, y solo el 20,5 % lo ha hecho por contra reembolso. El 55% de los encuestados prefieren utilizar la tarjeta de crédito para adquirir bienes o servicios en las tiendas virtuales.

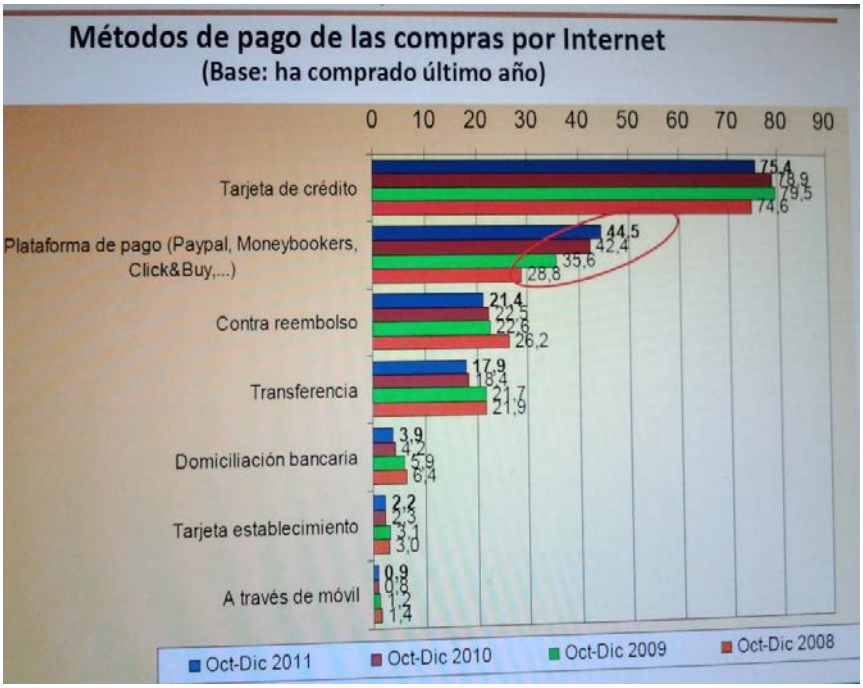
Grafico 2



Fuente: ONTSI

En este mismo sentido, la Asociación para la Investigación de Medios de Comunicación (AIMC) presentó en Madrid, el día 23 de febrero de 2012, los resultados de la 14ª encuesta a usuarios de Internet (Navegantes en la Red) realizada de octubre a diciembre de 2011[95]. Y según los resultados obtenidos por este mismo organismo, la tarjeta de crédito es el medio de pago más utilizado en la Red (75% de los usuarios). Por otro lado, diversas plataformas de pago (Paypal, Click&Buy, Moneybookers) siguen en alza y, con un crecimiento, se sitúan como segunda opción para el desembolso económico (44,5%) superando al contra reembolso (21,4%) y a las transferencias (17,9%). Sin embargo, el pago a través del móvil no termina de despegar y tan sólo es utilizado por el 0,9% de los encuestados. Obsérvese el Grafico 3

[95] AIMC. Publicado el 23 de febrero de 2012[En línea] disponible en Internet: http://download.aimc.es/aimc/f5g9/macro2011ppt.pdf (última consulta 21 de noviembre de 2012).



Fuente: AIMC

Como ya se señalaba con anterioridad, este medio de pago se encuentra escasamente regulado, tanto a nivel comunitario como a ni vel del ordenamiento jurídico español; es decir, muy pocos países han legislado sobre la materia, lo que dificulta su definición y clasificación en el marco jurídico. Sin embargo, debemos apoyarnos en la autonomía de la voluntad, como base de la contratación en el derecho español, según lo previsto en el art.1255 C. Civil, como desarrollaremos en el capítulo III.

En definitiva, conviene señalar que la diversidad de tarjetas electrónicas de pago existentes, unida a la amplia gama de servicios que ofrecen y a la continua incorporación de otros nuevos, hacen difícil el intento de delimitar el contenido del concepto genérico de “tarjeta electrónica de pago”.

1.5.1. Concepto de tarjeta electrónica de pago

Resulta difícil definir un concepto de tarjeta de pago, sobre todo por la variedad de las modalidades existentes, unido a la amplia gama de servicios que ofrecen y a la continua incorporación de otros nuevos. Sin embargo, la existencia de un elemento común a todas ellas permitió a la doctrina dar un concepto amplio que abarca las distintas modalidades de tarjetas que existen en la actualidad[96].

Algunas posturas doctrinales consideran que la tarjeta de pago no es más que un instrumento que surge a raíz de un contrato entre el titular y la entidad emisora de la misma en el que se recogen todas las condiciones de uso de la tarjeta[97]; es decir, se trata de un documento puramente probatorio que faculta a su titular a presentarlo ante un comerciante[98]. Para algunos, además es un documento materializado en un soporte de plástico con una banda magnética o un chip informático (microprocesador que contiene los datos personales y contables)[99]

[96] En la doctrina, BERNAL JURADO, plantea que "independientemente de los servicios que incorpore una tarjeta, todas tienen como objetivo identificar a su emisor y a la persona autorizada para su uso, bien cuando se realizan transacciones en las que se produce o aplaza un pago, o bien para facilitar la realización de cualquier otra operación financiera", BERNAL JURADO, E. *El mercado español de…*op., cit., p. 52; y por otro lado, los autores CARRASCOSA LÓPEZ; POZO ARRANZ; Y RODRIGUEZ DE CASTRO, definen la tarjeta, como aquel "documento mercantil, instrumental y electrónica, que permite a su titular, mediante compromiso contractual con el emisor, servir como medio de pago, a las vez que beneficiarse de una línea de crédito, limitada, que podrá utilizar en la compra de bienes o servicios, en establecimientos adheridos al sistema, o en el acceso a cantidades limitadas de dinero en bancos o entidades financieras que hayan concertado el servicio", en CARRASCOSA LÓPEZ; V POZO ARRANZ.; M.ª A; Y RODRÍGUEZ DE CASTRO, E.P. La *Contratación...*op., cit., p.42.

[97] JIMÉNEZ SÁNCHEZ, Guillermo. *Lesiones de Derecho Mercantil,* 4. ª ed. Madrid: Tecno, 1997, p. 347; GÓMEZ SÁNCHEZ, Amelia. *El sistema de tarjeta de crédito*. Granada: Comares, 2006, p. 2; MORENO NAVARRETE, M. A.: *Derecho-e. Derecho del comercio electrónico*. Madrid: Marcial Pons Ediciones Jurídicas y sociales S.A., 2002, pp.122 y ss.

[98] MARÍO GOFFAN, Carlos. *Tarjetas de Crédito. Análisis contractual, problemática procesal y penal.* Buenos Aire: Abeledo-Perrot, 2000, p. 12.

[99] Como señala GETE-ALONSO y CALERA, María Del C. *Las tarjetas de Crédito. Relaciones contractuales y conflictividad.* Madrid: Marcial Pons, 1997, p.11, cuando una tarjeta lleva chip informático, es cuando se trata de una tarjeta inteligente; BELTRÁN

La tarjeta «es un documento de plástico que incorpora una serie de datos: número de identificación personal (NIP) en la banda magnética o chip o también recientemente las tarjetas cuya lectura es "por proximidad", nombre de la tarjeta, de su emisor o gestor o de ambos, nombre del titular, firma del mismo, fecha de caducidad, etc.; además permite a su titular obtener bienes o servicios sin tener que efectuar su pago inmediato»[100].

En palabras de otros autores es «un negocio jurídico formal y complejo de crédito, plurilateral, de constitución sucesiva, múltiple, integrado por adhesión y de cumplimiento continuado, diferido y/o periódico»[101]. Hay quien la define «como un sustitutivo del dinero y como tal, es un medio de pago que se formaliza con firma en su sistema convencional de tipo asociativo o de adhesión y crediticio en cuanto a su convertibilidad en dinero»[102].

También hay quien la define como "documento privado de carácter mercantil, cuyo contenido esencial son los datos identificadores del propio

---

SÁNCHEZ, Emilio. M. y ORDUÑA MORENO, J (dirs.). *Curso de…op., cit.,* p. 273; en esta línea, el profesor VICÉNT CHULÍÁ la define como «un documento de material plástico resistente que permite el titular adquirir bienes y servicios (no dinero como el cheque), sin efectuar el pago inmediato», *en* VICENTE CHULÍÁ, Fco. *Compendio critico de Derecho Mercantil*, 2. ª ed. t II. Barcelona: Bosch, 1986, p. 967; por su parte en la doctrina italiana DI MARCHI, la define como "un documento que legitima al poseedor previa simples imposición de una firma sobre la factura o documento contable similar adquirir a crédito en los establecimientos asociados, mercancías y servicios, a cuyo pago queda obligado el remitente de la carta ", DI MARCHI, Giorgio, «Carte di crédito e carte bancarie», en *Banca Borsa e Titoli di Credito,* III. Milán: 1970.

[100] GÓMEZ MENDOZA, M. "Tarjetas bancarias", en GARCÍA VILLAVERDE, Rafael (dir.). *Contratos bancarios*. Madrid: Civitas, S.A., 1992, p. 373; GÓMEZ MENDOZA, M. *"Consideraciones en torno a las tarjetas de crédito", en Homenaje a Joaquín Garrigues,* t II. Madrid: 1971, p. 391*;* véanse BROSETA PONT, Manuel; MARTÍNEZ SANZ, Fernando. *Manual de Derecho Mercantil, Contratos mercantiles derecho de los títulos valores. Derecho concursal,* 12ª. ed. Madrid: Tecnos, 2005, p. 238; también, *Manual de Derecho Mercantil, Contratos mercantiles derecho de los títulos valores. Derecho concursal,* v II, 11ª. ed. Madrid: Tecnos, 2004, p. 231; véanse LÓPEZ PASCUAL, Joaquín y SEBASTIÁN GONZÁLEZ, A. *Gestión bancaria…*op., cit*.,* p. 315; ANDREU MARTI, María José. "Consideraciones en entorno al pago con tarjetas electrónicas, en *Estudios sobre el Consumo*, núm. 33, 1995.

[101] MUGUILLO, Roberto A. *Tarjeta de crédito. Régimen legal. Doctrina. Jurisprudencia*. Prólogo de Fernando M. Macheroni. Buenos Aires: Editorial Asterea, 1988, p. 15.

[102] LINARES BRETÓN, Samuel F.: *La tarjeta de crédito, su clasificación jurídica como medio de pago*. Buenos Aires: p. 144.

documento, de la entidad emisora y su titular, extendido sobre un soporte de material plástico rígido, al que en algunos casos, se incorpora una banda magnética para su lectura por medios electrónicos, cuyo objeto es permitir a su titular realizar diversas transacciones comerciales, utilizándola como medio u orden de pago"[103].

Tras analizar las diversas definiciones sobre el concepto de tarjeta de pago, entre otras, han de extraerse las siguientes conclusiones:

La tarjeta de pago es un medio de pago electrónico que permite a su titular obtener bienes o servicios sin tener que efectuar pagos en efectivo. Además, es un medio de pago electrónico que surge del contrato firmado entre la entidad bancaria y el titular de la tarjeta en el que se recogen todas las condiciones del funcionamiento de la tarjeta unidos a otros contratos necesarios que hacen posible su funcionamiento y que estudiaremos en el Capítulo III. También, las tarjetas pueden incorporar una banda magnética o un microprocesador en los que pueden figurar datos relativos a la identidad del titular (nombre y apellidos relieve), de la entidad emisora de la tarjeta y del número de cuenta, a los límites de crédito y disponibilidad y a la clave numérica secreta, cuando existe.

[103] INFANTE PÉREZ, V. «Tarjeta de crédito: su estudio jurídico», *Boletín del Ilustre Colegio de Abogado de Madrid,* núm.6. Madrid: 1989, p. 32; en este mismo sentido VICENT CHULÍÁ, F.: *Compendio critico de…*op., cit.; véanse GÓMEZ MENDOZA, quien la define como "aquel documento de plástico que incorpora una serie de datos número de identificación personal (NIP, PIN) en la banda magnética, nombre de la tarjeta, de su emisor o gestor o de ambos, nombre del titular, firma del mismo fecha de caducidad", GÓMEZ MENDOZA, "Tarjetas…"*op., cit*., p. 373; por su parte GÓMEZ PORRÚA, J.:"La tarjeta…"*op., cit.,* p. 189, considera la tarjeta como "un documento, de tamaño reducido y de fácil manejo, que actúa como título de legitimación, permitiendo a su titular obteniendo bienes o servicios sin necesidad de realizar su pago inmediato en dinero, limitando este en el momento de adquisición a la firma de una factura o nota de cargo, que será presentada por el establecimiento suministrador al emisor de la tarjeta, que abonará su importe y lo cargará posteriormente en la cuenta que mantiene con el titular"; como indica DAVARRA RODRÍGUEZ, la tarjeta de crédito es un "documento mercantil, instrumental y electrónica, mediante el que su titular tiene acceso a una línea de crédito asociado a la relación contractual previamente acordada", en DAVARRA RODRÍGUEZ. M. A. *Derecho informático.* Madrid: p. 268.

Al mismo tiempo, existen tarjetas que llevan incorporada foto de su titular con el objetivo de evitar el uso fraudulento de la misma[104]. Además, la tarjeta es un documento mercantil con características propias que puede cumplir diversas funciones que se concretan en lo que, desde el punto de vista económico, se conoce como los usos de las tarjetas[105].

1.5.2. Clasificación de las tarjetas electrónicas

Las tarjetas electrónicas de pago pueden ser clasificadas en distintas modalidades. La clasificación más usual de las tarjetas de pago se basa, como punto de partida, bien en el número de relaciones jurídicas que se producen en ellas (número de sujetos) o bien en el carácter de las relaciones jurídicas según la calificación de la operación (económica-jurídica) que cubren. Sin embargo, nos vamos a ocupar directamente del estudio de las tarjetas electrónicas que se utilizan para efectuar pagos en la red.

Veamos a continuación las diversas tipificaciones que da la doctrina sobre tarjeta electrónica.

1.5.2.1. *Por los elementos personales que intervienen*

De acuerdo a los sujetos intervinientes, se distingue entre tarjetas bilaterales, tarjetas trilaterales y multilaterales[106].

---

[104] Vid. La tarjeta de Caja Madrid (actualmente Bankia) de la Universidad Carlos III de Madrid.

[105] RIVERO ALEMAN, Santiago. *Disciplina del crédito bancario y protección del consumidor. (Cap. V. El crédito y el uso de medios electrónicos)*. Pamplona: Aranzadi, 1995, pp. 490 y ss; ajuicio de BARUTEL MANAUT, la tarjeta es un documento mercantil de ejecución de ese contrato intransmisible, que legitima a su titular para el ejercicio de derecho a que se le acepte la tarjeta como instrumento de pago, en BARUTEL MANAUT, C. *Las tarjetas de Pago y Crédito*. Barcelona: Bosch, 1997, p. 8.

[106] Según la clasificación que da la Audiencia Provincial de Pontevedra (Sección 1ª) en su sentencia de 29 julio de 2005, las tarjetas (...) pueden, "clasificarse en dos grupos: tarjetas de crédito bilaterales y trilaterales. Las primeras se entregan por determinados grandes almacenes o empresas a sus clientes como título que les legitima para utilizar los servicios de la cuenta corriente comercial abierta por los aludidos centros, mientras que las tarjetas trilaterales son aquellas en las que entre la entidad comercial y el propio cliente se interpone la entidad crediticia emisora de la tarjeta, que media en los pagos del propio cliente,

A. Tarjetas bilaterales

En las tarjetas bilaterales[107], la relación jurídica se establece entre la entidad emisora de la tarjeta y el titular de la misma. Podemos citar como ejemplo de este tipo de tarjetas las que son privativas, emitidas por los establecimientos comerciales, también denominadas tarjetas comerciales. Suelen ser de crédito o de pago diferido.

B- Tarjetas trilaterales

Hablamos de este tipo de tarjeta[108] cuando hay tres sujetos como mínimo: la entidad emisora y/o gestora de la tarjeta, el titular de la tarjeta y los establecimientos o personas que aceptarán la tarjeta como medio de pago[109].

Por lo que, van a surgir tres tipos de relaciones contractuales: un contrato entre la entidad emisora y/o gestora de la tarjeta y el titular de la tarjeta, otro contrato entre la entidad emisora y/o gestora y el establecimiento que se adhiere al sistema, y, por último, el contrato de cambio, en la que el

asumiendo frente a la entidad comercial el compromiso de atender el importe de los servicios o bienes adquiridos, de manera que cumplen una doble función: de un lado, constituyen instrumentos de pago que efectúa el Banco emisor respecto de la entidad comercial que prestó los servicios o entregó los bienes, y, de otro lado, comportan la apertura de crédito por la entidad bancaria a favor del titular de la tarjeta, de forma que la relación ya no se desarrolla entre el establecimiento comercial y el cliente, sino a tres bandas (incluso más, si la entidad emisora de la tarjeta es distinta del propio banco en que el que se concede el crédito y se domicilia el pago)", JUR/ 2006/ 21845.

[107] Vid. BOQUERA MATARREDONA, Josefina. "El impago de la deuda por la entidad emisora de la tarjeta de crédito", en CUÑAT EDO, V. y BALLARÍN HERNÁNDEZ (dirs.). *Estudios sobre jurisprudencia bancaria.* Navarra, Aranzadi, 2000, pp. 387 y ss; BERNAL JURADO, E.: *El mercado español de*…op., cit., p. 55; GÓMEZ MENDONZA, M. "Tarjetas…"*op., cit.,* p. 334.

[108] BOQUERA MATARREDONA, J.: "El impago de…"*op., cit.*, p. 388. vid. GÓMEZ MENDONZA, M; "Tarjetas…"*op., cit*., p. 375, quien señala que en la práctica suelen intervenir dos entidades bancarias, una que es el Banco adquirente que firma el contrato de aceptación con el establecimiento adherido al sistema y abone las facturas que le presenta. Por lo que se habla de tarjeta cuadrilateral.

[109] BARUTEL MANAUT, C, *Las tarjetas de...op., cit.,* p. 109. este autor señala que si el titular efectúa la transacción en el establecimiento comercial emisora de la tarjeta, entonces la tarjeta es bilateral a pesar de haber sido emitido con fin trilateral.

titular de la tarjeta presenta al establecimiento en el momento y a los efectos del pago en cumplimiento de una obligación que tiene con este último[110].

1.5.2.2. *Por el emisor*

Según el emisor, las tarjetas pueden ser bancarias y no bancarias y financieras[111]. ¿En qué consiste cada una de ellas?

A. Tarjetas no bancarias (tarjetas de compra)

Son emitidas por establecimientos comerciales o por un grupo de establecimientos para uso exclusivo de sus clientes (por ejemplo, las tarjetas de El Corte Inglés)[112].

También dentro de las tarjetas no bancarias podemos distinguir entre otros dos grandes grupos: las tarjetas acreditativas y las tarjetas privativas o comerciales. Como se decía en los párrafos anteriores, las tarjetas no bancarias o de compra son aquellas creadas por empresas que se dedican, principalmente, a la explotación de un determinado negocio de distribución de bienes o prestación de servicios y que facilitan a su titular determinadas condiciones en orden al pago de los bienes y servicios que éste adquiera en sus establecimientos[113].

[110] GETE-ALONSO Y CALERA, M.ª C. *Las tarjetas de…op., cit.,* p.17.

[111] BARUTEL MANAUT, C. *Las tarjetas de…op., cit.,* pp.102 y ss; ARRILLAGA, José Ignacio de. «La tarjeta de crédito». *Revista de Derecho Privado,* núm. 65, septiembre. Madrid, 1981, 784-804, especialmente, pp.791 y ss.

[112] BARUTEL MANAUT, C. *Las tarjetas de…op., cit.,* pp. 50 y ss*;* La llamada tarjeta de pago diferido del Corte Inglés fue creada en 1967, y desde allí ha tenido una extraordinaria difusión en todos sus centros comerciales, es de ámbito nacional y sirve básicamente para realizar compras al contado y crédito en referida cadena de grandes almacenes; BERNAL JURADO, E. *El mercado español…op., cit.,* p. 55*.* GÓMEZ MENDONZA, M.ª, "Tarjetas…"*op., cit.,* p. 374.

[113] MARIÑO LÓPEZ, Andrés. *Responsabilidad contractual por utilización indebida de tarjeta de crédito*. Prólogo de GETE-ALONSO y CALERA, M.ª C. Buenos Aires: Abeledo Perot, 2004, p. 13.

B. Tarjetas bancarias

Son aquellas emitidas por un banco u otra entidad de crédito bajo su propia marca (por ejemplo, la tarjeta 6000 CECA) o bajo otra marca, en calidad de suscriptor de un contrato de franquicia directo o a través de una entidad intermediaria (por ejemplo, la tarjeta Visa)[114]. Aquí el rol del emisor de la tarjeta y el gestor de la misma coinciden. Sin embargo, en las no bancarias veremos que estas figuras no coinciden.

C. Tarjetas financieras

Son aquellas que son emitidas por entidades no bancarias ni comerciales (por ejemplo, las T&E como Diner's Club, American Express), propietarias de una marca de tarjeta que acuerdan con establecimientos oferentes de bienes y servicios y con entidades bancarias la admisión de las mismas para efectuar el pago de las compras realizadas por el titular o, en el caso de las entidades bancarias, el suministro de efectivo a éste[115].

1.5.2.3. *Por el sistema de liquidación utilizado*

A. La tarjeta de crédito

La tarjeta de crédito[116] es un instrumento de pago mediante el cual la entidad emisora y/o gestora se compromete frente al titular de la tarjeta de

[114] BARUTEL MANAUT, una de las características que distingue la tarjeta bancaria del resto es la amplia gama de servicios que brinda a sus titulares cuando se utilizan en los sistemas de autoservicio bancario; las entidades de créditos pertenecen a las sociedades propietarias de la marca de la tarjeta con el único fin de servirse de la red de comunicaciones. La sociedad propietaria marca Visa, permite que una entidad de crédito, que previamente se ha constituido en socio suyo, emita la tarjeta sobre la que tiene derechos, siendo, en estos casos, el emisor de la tarjeta la entidad de crédito y haciendo la sociedad propietaria de la marca de las tarjetas las veces de entidad de franquicia BARUTEL MANAUT. C. *Las tarjetas de…op., cit.,* pp. 50 y ss; BERNAL JURADO, E. *El mercado…op, cit.,* p. 56; vid. GÓMEZ MENDONZA, María; "Tarjetas…"*op., cit*., p. 374.

[115] BERNAL JURADO, E. *El mercado español de tarjetas…op., cit.,* pp. 55 y ss.

[116] Véanse a RAMOS HERRANZ, I, y VILLAGOMEZ RODIL, A. (dirs.) *Contratos mercantiles especiales.* Madrid: Consejo general de poder judicial, 1997; GÓMEZ

crédito no sólo a concederle crédito, sino también a pagar las facturas por las compras realizadas mediante el uso de la misma en un establecimiento adherido al sistema y a prestarle otros servicios complementarios[117].

La particularidad de este tipo de tarjetas es que no se fija exactamente la cuantía del crédito, sino un límite máximo[118] de disponibilidad que no debe sobrepasar el titular durante un período de tiempo determinado. Durante ese período, el titular podrá efectuar pagos en establecimientos comerciales y obtener dinero a través de la red de cajeros automáticos. Tras finalizar el mismo, el titular de la tarjeta electrónica de crédito deberá reintegrar a la entidad emisora y/o gestora de la tarjeta la cuantía del crédito dispuesto.

La forma de pago de la deuda adquirida durante el tiempo pactado es la estipulada en el contrato, siendo común que se pacte la liquidación de la deuda de una sola vez, no estando, en ese caso, obligado al pago de

---

MENDONZA, María; "Tarjetas de…"*op., cit.,* p. 378; vid. BROSETA PONT, M; MARTÍNEZ SANZ, F.: *Manual de Derecho…*op., cit., p. 231.

[117] Véanse la Comunicación de la Comisión al Consejo Europeo: Una nueva baza para Europa: las tarjetas de pago electrónicas, COM (1986), 754 final, doc. cit. en su (anexo, punto 4.1), define «la tarjeta de crédito como aquella que permite que su portador se beneficie de una línea de crédito que le permite que su portador se beneficie de una línea de crédito que le permite comprar bienes y servicios hasta un límite preestablecido(derivado de un acuerdo entre el emisor y el poseedor de la tarjeta)»; DAVARA RODRÍGUEZ define a la tarjeta de crédito como "documento mercantil, instrumental y electrónico, mediante el que su titular tiene acceso a una línea de crédito asociado a una relación contractual previamente acordada", en DAVARA RODRÍGUEZ, M. A. *Manual de Derecho Informático.* Pamplona: Aranzadi, 2001, pp. 293-305; GETE-ALONSO y CALERA, M. C *Tarjeta de*… op., cit., 17 p; GETE-ALONSO y CALERA, M. ª C. *El pago mediante*…, op., cit., p.51; BARUTEL MANAUT, C. *Las tarjetas de…op., cit.,* pp.144-147; PASTOR SEMPERE, M. *Dinero electrónico*…op., cit., 185 p; Vid. CARRASCOSA LÓPEZ, V; POZO, Mª. A., y RODRÍGUEZ DE CASTRO, E.: *La Contratación Informático: el Nuevo Horizonte Contractual. Los Contratos Electrónicos e Informática*. 2. ª ed. Granada: Comares, 1999, 98 p; NUÑEZ LOZANO, Pablo Luis. *Tarjeta de crédito*. Madrid: Consejo Económico y Social, 1997, pp. 32-33.

[118] PLAZA PENADÉS, señala que la tarjeta de crédito "opera anticipando cantidades también con un límite estipulado, que se cobran en un periodo posterior, con independencia de que haya o no saldo en el momento de anticipo del pago, pero debiendo existir saldo suficiente para hacer frente a los pagos realizados el día en que se liquidan todos los cargos para los que la tarjeta anticipó numerario, en PLAZA PENADÉS J. «El pago a través de redes de comunicación en el Derecho Español y comunitario», *Revista Electrónica de Derecho Informático,* núm. 23, junio de 2000, [En Línea] Disponible en Internet: http:// www.vlex.com/redi. (última consulta 20 de noviembre de 2012).

intereses. Otra fórmula de pago es el aplazamiento del mismo que se puede realizar mediante el reembolso mensual de una cantidad fija, pudiéndose estipular una cantidad mínima, o el pago de un porcentaje de la deuda pendiente.

No obstante, el aplazamiento de las cantidades adeudadas supone el pago de intereses elevados. La falta de pago puede ser causa de resolución del contrato, pudiéndose exigir el pago de la deuda pendiente, así como los gastos, comisiones e intereses moratorios ocasionados por dicho motivo.

B. Las tarjetas de débito

La tarjeta de débito es aquel instrumento de pago electrónico que permite el acceso a los fondos que su titular tiene depositados en una cuenta bancaria[119]. Contrariamente a las tarjetas de crédito, no se trata de acceder al crédito concedido por la entidad financiera sino de acceder a los fondos de que dispone en una cuenta bancaria que debe asociarse a la tarjeta de débito[120]. Si no existe saldo disponible en la cuenta o se exceden los límites estipulados para la operación, la tarjeta no permitirá el pago[121].

[119] Vid. CARRASCOSA LÓPEZ, V; POZO, Mª. A. y RODRÍGUEZ DE CASTRO, E.: *La Contratación….op., cit.,* p.98; BERNAL JURADO, E.: *El mercado español de*…op., cit., p.58; BROSETA PONT, M; MARTÍNEZ; SANZ, F.: *Manual de Derecho…*op., cit., p. 231.

[120] LA FUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., p. 227; vid. GÓMEZ MENDONZA, M. "Naturaleza jurídica de las tarjetas de crédito, sus clases y carga de la prueba en el supuesto de extracciones en cajeros automáticos", *Revista de Derecho Bancario y Bursátil (RDBB)*, núm. 54, abril-junio, 1994, p. 486; RAMOS HERRANZ, I. Medios de…*op., cit.,* p. 546; en el mismo sentido RICO CARRILLO, M. «El pago mediante tarjetas en el comercio electrónico a través de Internet», en *RCE,* núm.3, 2000, pp.3-44; por su parte la Comunicación de la Comisión al Consejo Europeo: Una nueva baza para Europa: las tarjetas de pago electrónicas de 12 de enero de 1987, en su (anexo, punto 4.2), define la tarjeta de debito como « aquella que da acceso a la cuenta bancaria del poseedor en la que repercutirán las operaciones realizadas mediante tarjeta(por lo general retirada de billetes de una ventanilla bancaria automática o pagos realizado en un Terminal instalado en el punto de venta) y esto se hará inmediatamente o (en caso de operaciones on-line) después de un periodo muy corto»; PASTOR SEMPERE, define a la tarjeta de débito como "aquella tarjeta electrónica que se encuentran vinculadas a una cuenta corriente o depósito que opera exclusivamente de forma electrónica y automática, y que las operaciones realizadas por el cliente son adeudadas inmediatamente en el caso que el terminal o el

Para algunos autores, la tarjeta de débito no es más que un "documento mercantil, instrumental y electrónico, mediante el que su titular tiene acceso a una cuenta corriente bancaria a la que está asociada y, en consonancia con ella, puede realizar operaciones cuyo pago atiende dicha cuenta."[122]

Con la tarjeta de débito[123] su titular puede realizar operaciones bancarias en relación con las cuentas que tenga en dicha entidad (extracción de dinero en efectivo en cajeros automáticos, realización de transferencias bancarias, recarga de teléfono móvil, compra por Internet, etc.), y utilizarla como medio de pago de bienes y servicios prestados por establecimientos adheridos al sistema.

1.5.3. *La diferencia entre las tarjetas de crédito y las de débito*

Una de las características que distingue la tarjeta de crédito de la tarjeta de débito es que aquella permite a su titular hacer uso de crédito, así como permitir que éste la utilice en un establecimiento adherido al sistema para la adquisición de bienes o servicios, en sustitución de un pago en dinero en efectivo[124].

El modo de funcionar de las tarjetas de débito es diferente al de crédito, ya que son un instrumento que permite a su titular producir un movimiento del saldo de su cuenta corriente, desencadenando automáticamente una

---

cajero esta conectados al ordenador central--operaciones *on line*-- o en caso contrario– operaciones *off line-",* en PASTOR SEMPERE, M. *Dinero electrónico*, op., cit., p.184.

[121] PLAZA PENADÉS, J. "El pago a través de…"*op., cit., p. 2.*

[122] DAVARA RODRÍGUEZ, M. A.: *Manual de...op., cit.*, p. 294.

[123] GETE-ALONSO, M. C. *Tarjeta de*…op., cit., pp. 18 y ss; MARIÑO LÓPEZ, A. *Responsabilidad contractual por utilización indebida de tarjeta de crédito*. Tesis Doctoral presentada en la Facultad de Derecho. Departamento de Derecho Privado. Universidad Autónoma de Barcelona, 2003, p. 13.

[124] Sobre este aspecto ver GUIMARAES, María Raquel. "El pago mediante tarjeta de crédito en el comercio electrónico. Algunos problemas relativos a su naturaleza jurídica, marco contractual y régimen aplicable, desde una perspectiva comparada en los derechos portugués, español y comunitario", en MATA Y MARTIN, M. Ricardo (dir.). *Medio electrónico de pago. Los problemas jurídicos*. Granada: Comares, 2007, p. 171; BROSETA PONT, M. MARTÍNEZ; SANZ, F.: *Manual de Derecho…*op., cit., p. 231.

transferencia electrónica de fondos. De este tipo de tarjeta se puede hacer uso tanto en un cajero automático como en un establecimiento comercial.

1.5.4. Tarjetas de prepago

Dentro de las tarjetas de prepago se pueden distinguir: las tarjetas de prepago de finalidad limitada y las tarjetas de prepago de finalidad múltiple. No obstante, nos interesa analizar la tarjeta de prepago de finalidad múltiple que es aquella que puede ser utilizada en los puntos de venta de varios proveedores de servicios para una multiplicidad de finalidades, lo cual tiene el potencial de ser usada a escala nacional o internacional, pero puede ser restringidos a ciertas áreas. Se efectúa una carga de dinero en la tarjeta y pueden realizarse operaciones hasta consumir el importe cargado[125].

El caso típico de la tarjeta de prepago lo constituye el monedero electrónico que hemos definido en el capítulo I, epígrafe 1.4.5. Cabe indicar que actualmente las tarjetas de prepago suelen emitirse en soportes físicos (tarjeta de plástico) con dimensiones similares a las tradicionales tarjetas de crédito o débito, a los que se ha incorporado un dispositivo electrónico para permitir el almacenamiento de información, y normalmente cuentan con un circuito integrado con capacidad de procesamiento de datos. Se dividen en dos categorías:

- *Las tarjetas con memoria simple (memory chip card):* son capaces de almacenar información pero no son capaces de procesarla. Es decir, son sólo dispositivos de almacenamiento de datos, y esta característica las hace muy similares a las tarjetas con banda magnética, en las que se aloja una cantidad limitada de datos, en un formato definido según el tipo de aplicación[126].

[125] Según entiende BERNAL JURADO, E. *El mercado español de*…op., cit., p. 56.

[126] En la actualidad existen dos tipos de tarjetas de memoria: las de un solo uso, para las que la aplicación más difundida es en el campo de la telefonía pública, donde se utiliza como tarjeta de débito de pulsos previamente cargados en la memoria. Cuando se utiliza la

- *Las tarjetas inteligentes (smart cart):* incorporan un microprocesador que les confiere una alta capacidad de memoria. Adicionalmente, están acompañadas de un procesador lo que les permite no sólo almacenar información sino que además pueden realizar un procesamiento de datos local y realizar cálculos con complicados algoritmos como los utilizados para el cifrado de datos (encriptación), permitiendo implementar avanzados mecanismos de seguridad contra los intentos de robo y fraude[127].

El uso de la tarjeta de prepago por parte de titular reduce la necesidad de llevar dinero en efectivo para pequeñas transacciones, disminuye el riesgo de robo si su utilización incluye un elemento de seguridad como el PIN y permite realizar pagos sin vinculación a una cuenta bancaria.

Para los proveedores de bienes o servicios ofrecen la ventaja de reducir los costes de entrega de efectivo y la desaparición del riesgo de que el pago sea rechazado por falta de fondos del titular; por otro lado ofrecen las oportunidades adicionales de realizar actividades promocionales basadas en la capacidad de memoria de esta tarjeta[128]. También este tipo de tarjeta evita la identificación del usuario y el acceso a la cuenta bancaria o a la tarjeta de crédito del mismo para verificar la disponibilidad de fondos, porque los únicos fondos disponibles son los que están en la tarjeta.

---

tarjeta los pulsos se descargan. Y la otra clase son las recargables, donde el uso más frecuente es en los denominados monederos electrónicos.

[127] Como señala, BERNAL JURADO, el microprocesador incorporado en este tipo de tarjeta tiene como funciones: estrictamente financiera (monedero electrónico) y la no financieras, reservados para aquellos servicios adicionales que el emisor de la tarjeta dese prestar a sus titulares, expedientes académicos (por ejemplo la tarjeta de Caja Madrid, de la Universidad Carlos III de Madrid, que tiene como finalidad el uso exclusivo de los servicios que presta la Universidad), o historial médico, en BERNAR JURADO, E. *El mercado español de*…op., cit., p. 57. nota 16.

[128] MARTÍNEZ NADAL, A. *El dinero*…op., cit., p. 17.

1.5.5. Tarjeta de cargo diferido o tarjeta de compra

Según se establece en el anexo, punto 4.4, de la Comunicación de la Comisión al Consejo de 12 de enero de 1987, es una tarjeta que es emitida por una firma comercial (empresas de distribución, hipermercados, Gasolineras, empresas de transporte, de alquiler de automóviles, etc.…). Podemos equipararla con las tarjetas de crédito con la diferencia de que el comerciante o prestador de servicios al que se presenta la tarjeta es al mismo tiempo el emisor y concede el crédito que se desprende de ella; la supuesta tarjeta no puede ser presentada para pago a otro comerciante[129].

La Recomendación de la Comisión 88/590/ CEE, de 17 de noviembre de 1988, define esta tarjeta en su anexo, punto 2, «como la emitida por un detallista destinada a su cliente, o por un grupo de detallistas para sus clientes, con el fin de permitir o facilitar, sin acceso a una cuenta bancaria, el pago de la compra de bienes o servicios adquiridos directamente del detallista o detallistas emisores, aquellos que en virtud del contrato acepta la tarjeta».[130]

Como hemos señalado con anterioridad, en las tarjetas no bancarias no coincide la persona del emisor y el gestor: el emisor suele ser un establecimiento comercial o un grupo de establecimientos y el gestor una entidad de crédito. Este tipo de tarjeta, al igual que las tarjetas de crédito, concede crédito a su titular pero se diferencian en la forma de liquidación del crédito y en el límite establecido. Es decir, no establece el límite de gastos,

[129] Vid. *Comunicación de la Comisión al Consejo de 12 de enero de 1987*, en la que refiere este tipo de tarjeta como la de cliente. Anexo, punto 4.4; según sostiene GETE-ALONSO, la conceptualiza como aquellas que son creada por empresas que se dedican, principalmente a la explotación de un determinado negocio y facilitan, a su titular determinadas condiciones en orden al pago de los bienes y servicios que se adquiera en su establecimientos, en GETE-ALONSO y CALERA, M. C. *Las tarjetas de*…op., cit., p.19; ejemplos de este tipo de tarjetas están las de Dinero Club; American Express; las tarjetas de Corte Inglés; Carrefour; y las de Al campo.

[130] la Recomendación de la Comisión 88/590/CEE, 1988; sobre este mismo punto ver GETE-ALONSO Y CALERA, M. *Las tarjetas de*…op., cit., p .19.

opera conforme a la acumulación de los pagos realizados para su cargo diferido al final del mes o en otro periodo o fecha, teniendo el titular que abonar mensualmente la totalidad de operaciones realizadas[131].

En conclusión, cabe reiterar que la tarjeta de crédito o débito es el medio electrónico de pago más conocido y utilizado por los consumidores y usuarios en el comercio electrónico. Todo esto, se debe básicamente a su comodidad, facilidad de uso, seguridad en las operaciones comerciales y financieras. Al mismo tiempo, elimina la necesidad de disposición de efectivo.

1.6. Sujetos que intervienen en el uso de tarjeta electrónica

Para comprender las diversas relaciones jurídicas existentes en una operación de pago electrónico mediante tarjeta de (crédito o débito), es imprescindible estudiar en este epígrafe los diversos sujetos intervinientes.

En el derecho español no existe una normativa jurídica que defina el concepto de titular de una tarjeta de pago, ni de emisor, ni de comerciante adherido al sistema o proveedor de bienes o servicios. Por tal razón nos apoyaremos en las distintas recomendaciones comunitarias existentes con el objetivo de definir cada uno de estos sujetos.

Pues bien, la multiplicidad de los sujetos intervinientes en las transacciones en la que se utilizan protocolos de seguridad (infra Cap. II, epígrafe 2.5), así como de los intermediarios encargados de suministrar los servicios informáticos, merece un estudio exhaustivo. Por tal motivo, en este epígrafe analizaremos todos aquellos sujetos que intervienen de una forma u

[131] PASTOR SEMPERE, M. *Dinero electrónico*, op., cit., p. 185; RICO CARRILLO, M., "El pago mediante tarjetas en el comercio electrónico a través de Internet", *RCE,* op., cit., pp. 17 y 18; GÓMEZ PORRÚA, J.M., "La tarjeta de crédito", en JIMÉNEZ SÁNCHEZ (coord.), *Derecho mercantil,* 7. ª ed. Barcelona: Ariel, S.A., 2002, p. 201.

otra en las transacciones en la que se utilizan los protocolos SET, SSL y 3 D Secure.

1.6.1. La entidad emisora y/o gestora de la tarjeta

En los distintos textos normativos que hemos analizado no hemos encontrado una definición general sobre la entidad emisora y/o gestora de la tarjeta[132], es decir, actualmente no existe una definición general aplicable a este sujeto interviniente en el pago electrónico; cada una de es tas normativas comunitarias han ido conformando la definición que mejor se acomoda a ellos.

Por lo que en la Recomendación 87/598/CEE, en su (aparto II, punto 2), se entiende por «emisor»: cualquier establecimiento de crédito u organización de t arjetas que expida tarjetas de pag o de uso electrónico, cualquier empresa de producción o de servicios que expida también tarjetas de este tipo.

[132] En la doctrina RODRÍGUEZ DE LAS HERAS BALLELL, señala que *"*es importante diferenciar el concepto de entidad emisora de la tarjeta y el de entidad gestora de la misma. En el caso de l as tarjetas bancarias, emitidas por una entidad de crédito coinciden las figuras de em isor de l a tarjeta y gestor de la misma. Por el contrario, en l as tarjetas comerciales o no ba ncarias, el emisor es un es tablecimiento comercial o u n grupo de establecimientos comerciales, mientras que la gestión de la tarjeta recae en una entidad de crédito. Posición que ha bíamos mantenido en los epígrafes anteriores que la figura de la entidad emisora y gestora coinciden", RODRÍGUEZ DE LAS HERAS BALLELL, T "El reparto de riesgo y la atribución de responsabilidad en el uso de tarjeta en la contratación electrónica", en R ICO CARRILLO, Mariana (coord.) *Derecho de las Nuevas Tecnologías*, Buenos Aires: la Roca, 2007, p. 330; por su parte BAUTECAS CALETRIO, señala "que puede ocurrir que el emisor de la tarjeta no sea a la vez el gestor de la misma, y esto daría lugar a cuatro sujetos y a cuatros relaciones jurídicas. Y que también puede ocurrir que el establecimiento comercial tenga su propia entidad de crédito que se encarga de gestionarle la domiciliación de los cobros provenientes de los pagos con tarjeta, lo que daría lugar la existencia de cinco participantes y a cinco relaciones jurídicas. Y que no obstante a eso, la mayoría de veces las entidades de créditos gestoras de las tarjetas son a la vez miembros de la sociedad emisora de las mismas", en B AUTECAS CALETRIO, A. *El pago electrónico...*, op., cit., p. 56; partiéndonos de este criterio, centraremos nuestro análisis en aquellos supuestos en la que la figura de la entidad emisor de la tarjeta sea al mismo tiempo la entidad gestora de la misma; vid., LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., p. 239; NUÑEZ LOZANO, P. L. *La tarjeta de…*op., cit., pp.34 y ss.

Por su parte, la Recomendación 88/590/CEE establece en su anexo 2 párrafo segundo que el «emisor es la persona que, en el marco de su actividad profesional, pone a disposición de un cliente un instrumento de pago, en virtud de un contrato suscrito con él».

De acuerdo al literal e) del art. 2 de la Recomendación 97/489/CE, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisor y titulares de tales instrumentos, el «emisor, es la persona que, en desarrollo de su actividad profesional, pone a disposición de otra persona un instrumento de pago en virtud de un contrato suscrito con él».

Hay quienes definen al emisor de la tarjeta como la persona jurídica que, en el marco de su actividad, emite la tarjeta de pago (propia o con marca de propiedad de otra entidad), poniéndola a disposición de sus clientes en virtud de un contrato suscrito con ellos para que éstos la utilicen como medio de pago en la adquisición de bienes o servicios, quedando obligada frente al establecimiento que facilita los bienes o servicios al pago del importe de la factura correspondiente[133].

Es decir, el emisor no es más que un empresario que crea la tarjeta de pago o crédito, hace la entrega a su titular y resulta obligado, fundamentalmente en el caso de bilateralidad, a permitir aplazar los pagos correspondiente a los bienes o servicios que adquiera u obtenga en sus propios establecimiento[134]; o una entidad que emite la tarjeta para su

[133] GÓMEZ PORRÚA, J. M., "La tarjeta…"*op., cit.,* pp. 192 y ss; GETE-ALONSO, M. C. *Las tarjetas de crédito…*op., cit., p.38; BERNAL JURADO, E.: *El mercado español de tarjeta…*op., cit., pp. 58 y ss; JAVIER CORTÉS, L. "Los Contratos bancarios (II)", en MENÉNDEZ, Aurelio (dir.). *Lecciones de Derecho Mercantil*, 3. ª ed. Navarra: Aranzadi, S.A., 2005, pp. 676-677.

[134] NUÑEZ LOZANO, P. L. *La tarjeta…*op., cit., pp. 34 y ss; Argentina: Ley 25.065 de tarjeta de crédito, publicado en *Boletín Oficial, el* 14 de enero de 1999, en su art. 2 a) define la entidad emisora como aquella entidad financiera, comercial o bancaria que emite tarjeta de crédito, o que haga efectivo el pago. [En línea] disponible en Internet.

utilización en establecimientos distintos con los que previamente ha suscrito un contrato.

1.6.2. Titular y/o contratante/solicitante

Nos parece interesante distinguir estas figuras, ya que en la literatura no es fácil determinar claramente quién es titular de una tarjeta, si una persona puede ser titular y al mismo tiempo solicitante o si debe tratarse de dos personas distintas. Todo esto ha originado confusión a la hora de definir el concepto.

En nuestra opinión, el titular de la tarjeta es la persona física o jurídica a cuyo nombre se expide la tarjeta; y que una vez aceptada la solicitud de concesión de tarjeta por el solicitante comprometido al pago del crédito, la entidad de crédito le autorizará para utilizarla en virtud del contrato.[135]

Cuando hay confusión entre titular y contratante son ambas personas quienes asumen tanto las obligaciones como los beneficios derivados de la tarjeta de crédito. Y en el caso de que no se llegue a producir esta confusión, o que no sea absoluta, se distinguen dos supuestos[136].

Primero: cuando el titular es a su vez contratante pero designa a otras personas para que puedan utilizar la tarjeta, hay que distinguir entre titular básico o contratante y titulares autorizados o beneficiarios[137].

---

http://www.adecua.org.ar/legislacion.php?ver=bancos_25065 (última consulta 16 de noviembre de 2012)

[135] Ved. Recomendación 97//489/CE; en la doctrina GETE-ALONSO, mantiene que el titular va ser siempre una persona física, aun cuando la tarjeta se haya expedido para llevar a cabo pagos de la empresa u organismo en la que el presta su servicios bajo relación laboral, profesional o funcional, *en* GETE-ALONSO, M. Carmen. *Las tarjetas de crédito…op., cit.,* 39 p*;* FERNANDEZ ORENES, F.; y VILLALOBO RUÍZ, D. *La tarjeta de*…op., cit., pp.144 y ss; BERNAL JURADO, E. *El mercado español*…op., cit., p. 59.

[136] GÓMEZ PORRÚA, J. M. "La tarjeta de crédito…"*op., cit*. pp. 192 y 193.

[137] BARUTEL MANAUT señala que el titular contratante, es aquel titular que ha contratado, con la debida representación legal, pero no puede utilizar por sí mismo la tarjeta de pago, ya sea por imposibilidad física como es el caso de las personas jurídicas, o por

Un único contrato da lugar a la emisión de varias tarjetas tanto a favor tanto del contratante como de sus beneficiarios, pero aquellas obligaciones que se derivan de las tarjetas de crédito (reintegro de las cantidades dispuestas, pago de cuotas de suscripción o periódicas) son asumidas exclusivamente por el titular básico o contratante, no así sus beneficios que se derivan tanto para él como para las personas por él designadas como beneficiarios.

Segundo: cuando el contratante no es titular, designando a otra u otras personas como beneficiarios, las obligaciones son asumidas por aquél, en tanto que los beneficios de la tarjeta redundan en estos últimos, como sucede en las tarjetas de empresas solicitadas por éstas para sus directivos o empleados.

1.6.3. Proveedor de bienes o servicios adherido al sistema de pago con tarjetas

Algunos autores definen al establecimiento o prestador de bienes o servicios como aquellas personas físicas o jurídicas que, en virtud del acuerdo establecido con el emisor de la tarjeta, aceptan en su establecimiento la tarjeta como medio de pago de los bienes o servicios que adquieren los titulares de las mismas, ya sea on line u off line[138]. Por lo que

incapacidad jurídica, como es el caso de los incapacitados. BARUTEL MANAUT, C. *Las tarjetas de*…op., cit., p. 245; el art. 2 b) de la *Ley 25 de tarjeta de crédito de Argentina*, define el titular de la tarjeta de crédito: como aquel que está habilitado para el uso de la tarjeta de crédito y quien se hace responsable de todos los cargos y consumos realizados personalmente o por los autorizados por el mismo; y en su inciso c) define al usuario, titular adicional, o beneficiario de extensiones: aquel que está autorizado por el titular para realizar operaciones con Tarjeta de Crédito, a quien el emisor le entrega un instrumento de idénticas características que al titular.

[138] En este sentido NUÑEZ LOZANO, la define como aquel establecimiento que acepta como medio de facilitación de los pagos correspondiente a los bienes o servicios propios del objeto de su trafico la utilización de las tarjetas de crédito pertenecientes al mismo sistema y consecuente mente deviene beneficiario de las órdenes de pago girado a tal efecto a cargo del emisor por los titulares de las tarjetas, en NUÑEZ LOZANO, Pablo. *La tarjeta de crédito*. Madrid: Colección de Estudios, 1997, pp. 46 y ss.; vid. DAVARA RODRÍGUEZ, M. A. *Derecho*…op., cit., p. 284; vid. JAVIER CORTÉS, L. "Los Contratos…"*op., cit.,* pp. 677 y ss;

garantizará el servicio al titular de la tarjeta, habilitando un terminal de punto de venta (TPV) compatible con el sistema al que se haya adherido el mencionado establecimiento, si bien este extremo no plantea mayores problemas por cuanto en la práctica es la entidad financiera (emisora de la tarjeta o autorizada por la entidad titular de la marca del medio de pago) la que procede a instalar el TPV en el establecimiento comercial.[139]

Dentro del entorno del comercio electrónico encontraremos estos proveedores a través de la red en los sitios web que éstos habilitan para prestar sus servicios por vía electrónica[140]. Es la persona física o jurídica que ofrece sus productos o servicios en su página web a cambio de pago con tarjeta como medio de pago electrónico, que es gestionado por su entidad financiera (adquirente) a través de "pasarela de pagos". Existe una relación contractual entre el proveedor y la entidad emisora de la tarjeta que obliga a aquel a aceptar la tarjeta como medio de pago; también pueden concurrir en la misma persona ambas condiciones, es decir la figura de entidad emisora y de proveedor[141].

1.6.4. Entidad adquirente

Es la entidad de crédito o financiera con la que el proveedor de servicios o bienes (establecimiento comercial) firma un contrato de aceptación de la

---

En el Derecho Argentino la Ley 25/ 0.65 de tarjeta de, en su art. 2 f) define Proveedor o Comercio Adherido: aquel que en virtud del contrato celebrado con el emisor, proporciona bienes, obras o servicios al usuario aceptando percibir el importe mediante el sistema de Tarjeta de Crédito; hemos mencionado esta legislación por considerarla una de las normativas pioneras del mundo en regular el contrato de tarjeta.

[139] LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., pp. 245 y ss.

[140] Ibídem, pp. 240 y ss.

[141] según sostiene LAFUENTE SÁNCHEZ, este tipo de supuesto se da en aquellos casos en la que el emisor de la tarjeta es una entidad financiera que, a su vez, actúa como proveedor cuando su titular utiliza la misma en un cajero automático de la propia entidad. De igual forma cuando el emisor sea un establecimiento comercial que expide tarjetas electrónicas (por ejemplo, El Corte Inglés) y posteriormente el titular de la misma la utiliza para adquirir un bien o servicios en el establecimiento, sobre este mismo caso podemos hablar de las tarjetas de Al campo, entre otras., LAFUENTE SÁNCHEZ, R, *Los servicios financieros…op., cit.,* p. 240, nota al pie 556*;* PLAZA PENADÉS, J. "Contratación electrónica…"*op., cit*., p. 455.

tarjeta, donde presentará cobro y se ordenará el abono automático de todos los importes correspondientes a las transacciones con tarjeta electrónica[142].

La figura de esta enditad de crédito puede coincidir con la del emisor, aunque en la práctica es muy difícil que suceda, dada la diversidad de emisores y aceptantes de la tarjeta. En otras palabras, podemos definir a la entidad adquirente o banco adquirente como aquel banco que actúa en nombre del proveedor de servicios o bienes (establecimiento comercial) y se encarga de autorizar y procesar los pagos efectuados mediante tarjeta a través del sistema de pasarela de pagos[143].

1.6.5. Entidad franquiciadora

Es la propietaria de la marca de la tarjeta de crédito que autoriza al emisor a poner en circulación en un país determinado o en una zona determinada, con carácter exclusivo o compartido, la referencia de la tarjeta de crédito (ejemplo Visa internacional)[144]. Como decíamos anteriormente, el emisor franquiciador es el propietario de la marca de tarjeta de crédito que otorga licencia a entidades financieras miembros de su sistema para emitir este medio de pago a particulares y empresas y celebrar contratos con comercios que desean adherirse al sistema de pagos[145].

1.7. Intermediarios

Para referirnos a los intermediarios que intervienen en la operativa de pago en el comercio electrónico es necesario, en primer lugar, definir en qué

[142] vid BARUTEL MANAUT, Carles, *Las tarjetas de pago y crédito*, op., cit., 244 p; GÓMEZ SÁNCHEZ, A. *El sistema…op., cit.,* p. 13.

[143] vid. LAFUENTE SANCHÉZ, R. *Los servicios financieros*…op., cit., p .240.

[144] Ejemplo de la entidad de franquicia podemos citar Visa, que cede los derechos de explotación a cada entidad de crédito que, a su vez, son sus socios. No se debe confundir la relación existente entre la entidad de franquicia y las entidades emisora de la tarjeta, con la relación existente entre las entidades de crédito emisora de la tarjetas y otras entidades de crédito que pueden actuar como corresponsales suyos para efectuar algunas operaciones.

[145] LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., p. 245; BARUTEL MANAUT, C. *Las tarjetas de*…op., cit., pp. 244 y ss.

consiste el servicio de intermediación para luego estudiar los distintos intermediarios que intervienen en el comercio electrónico.

Podemos comenzar diciendo que el servicio de intermediación[146] es aquel servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información. Esto quiere decir que la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicación, el alojamiento de datos en los propios servidores o, entre otros, el acceso o recopilación de datos o de enlaces a otros sitios de Internet,[147] son servicios de intermediación. Un servicio de intermediación ha de ser, en primer término, un servicio de la sociedad de la información, es decir, ha de ser un servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario[148].

[146] Refiriendo al concepto de intermediario dentro del ámbito de la contratación electrónica, ILLESCAS ORTIZ, R. *Derecho de…*, op., cit., pp.131-132, para este autor la palabra intermediario no es la más apropiada para designar esta pléyade de empresarios o propietarios de redes interconectadas, así como de los prestadores de servicios relacionados con el comercio electrónico. Es la industria quien acabó por imponer dicha denominación genérica para designar a todos cuantos intervienen en el comercio electrónico a titulo distinto del de contratantes–iniciadores destinatarios de los MD, contractuales--. Desde una perspectiva jurídica, en efecto, las actividades desempeñadas por unos y otros son muy distintas entre sí, el régimen de la responsabilidad que les afecta no es homogéneo y lo más relevante es que ninguno lleva a cabo funciones de intermediación entre los contratantes en el sentido técnico-jurídico del término; a juicio de PLAZA PENADES, la expresión "intermediario" en relación con un mensaje de datos se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él", PLAZA PENADES J. "Responsabilidad civil de los intermediarios en Internet", en GARCÍA MEXIA, Pablo (dir.). *Principios de derecho de Internet*, Valencia: Tirant lo Blanch, 2005, pp. 399- 400; vid. RODRÍGUEZ DE LAS HERAS BALLELL, T, «El tercero de confianza en el suministro de información. Propuesta de un modelo contractual para la sociedad de la información», en *Anuario de Derecho Civil,* Tomo LXIII, Fascículo III, 2010, pp. 1245-1284.

[147] Ver el inciso b) del anexo de la LSSICE; vid. GRAMUNT FOMBUENA, Mª. Dolors. "El estudio jurídico…"*op., cit.,* pp.17-18; CARANCHO HERRERO, Mª. Teresa. "Breve apunte sobre la responsabilidad de los prestadores de servicios de intermediación", en MURRILLO VILLAR, Alfonso y BELLO PAREDE, (coords.). *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*. Burgos (España): 2005, pp. 202-203.

[148] PAYERAS CAPELLA, M. "Los servidores de acceso y alojamiento: descripción técnica y legal", en CAVANILLAS MÚGICA, S (coord.). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*. Granada: Comares, 2005,

Como pone de relieve algún autor "los intermediarios solventan los fallos del mercado a través de las siguientes funciones: agregación, credibilidad facilitación de las relaciones y Matching"[149].

---

p. 22.

[149] Suscribiendo textualmente la tesis sostenida por la Profesora RODRÍGUEZ DE LAS HERAS BALLELL, quien subrayar las siguientes funciones de l os intermediario: a) *agregación:* la intermediación reduce - hasta m + n - las múltiples relaciones (m x n) entre (m) compradores y (n) vendedores transformándolas en relaciones bilaterales a través de su mediación, es decir, centralizándolas. Consecuentemente, se reducen los costes de transacción, permitiendo el aprovechamiento de las economías de escala. Esta función es destacable en los modelos de agregación como los supermercados financieros o los *one-stop-shopping*; b) *Credibilidad:* los intermediarios desempeñan una labor esencial de dotación de confianza a las transacciones en entornos con asimetrías de información. La dificultad de los compradores para discriminar los productos por su calidad y los vendedores por su credibilidad es origen de un fallo en el mercado, fuente de una externalidad que da lugar a comportamientos oportunistas situación de divergencia de incentivos típica de una relación de agencia o de disparidad de información sobre la calidad propia de un mercado de "cacharros" – (*markets for "lemons"*)-.

La figura de los intermediarios representaría así un mecanismo del mercado en sectores donde los operadores tiene dificultades para construir su reputación. En una situación de competencia entre intermediarios, será la reputación de éstos la que permita la discriminación de los compradores, produciendo así una transferencia de reputación de los vendedores a los intermediarios. Además, los intermediarios pueden contribuir a un reparto más eficiente del riesgo, asumiendo su parte en las relaciones compradores-intermediarios-vendedores. Los portales, los anuarios especializados o el empleo de la técnica de enlaces transmiten al usuario un factor añadido de credibilidad. A su vez, en la competencia en el mercado, estos intermediarios compiten entre sí con elementos reputacionales, es decir, fiabilidad, profesionalidad, especialización, orientación ideológica o política, que ponen de manifiesto a través de "señales", prácticas, estrategias o comportamientos que tratan de reajustar la toma de decisiones en el mercado al transmitir información adicional sobre la calidad –garantías, compromisos, asunción de responsabilidad -Los servicios de certificación y sello de garantía, las diversas modalidades de rating tanto en entornos abiertos como cerrados (como mecanismo de "autocontrol" en redes sociales, redes P2P, plataformas de contratación o subastas electrónicas) representan la intermediación por generación de confianza, esto es, prestar servicios dirigidos a reforzar la credibilidad.

Por otra parte destaca que la reputación adquiere una importancia esencial en la creación de incentivos. De un lado, dada la asimetría de información del mercado, la reputación actúa como función de "garantía" frente al demandante, facilitando la labor de búsqueda, selección y elección. De otro, la reputación se erige como barrera a la entrada en el mercado, su mantenimiento reduce la extensión subjetiva de la competencia y, sobre todo, garantiza la adquisición de beneficios conocidos como "rentas derivadas de la reputación". En un mercado con información imperfecta donde el mecanismo de la reputación desplaza el criterio de elección a la calidad, el precio se sitúa por encima del coste marginal. En el mantenimiento de este margen se encuentra el origen de tales beneficios y en éstos, los incentivos de los oferentes para cultivar su buena reputación". *c) Facilitación de las relaciones* los intermediarios facilitan la interacción entre compradores y vendedores coordinando el proceso de intercambio de información, que es un proceso costoso, "traduciendo" – es decir, adaptando, añadiendo valor – la información,

1.7.1. Proveedores de acceso

Son los intermediarios que facilitan el acceso a una red de telecomunicaciones[150], por ejemplo la red Internet. En la Ley 34/2002, de servicio de la sociedad de información y comercio electrónico, de 19 de junio de 2002 (LSSICE), se plantea que estos prestadores de s ervicios de transmisión y concesión de acceso no dejan de ser intermediarios (mere conduit) por el hecho de que incluyan el almacenamiento automático, provisional y transitorio de los datos transmitidos, siempre que el mencionado almacenamiento sirva exclusivamente para ejecutar la transmisión y que su duración no sea superior al tiempo necesario para su transmisión(art.14)[151].

1.7.2. Proveedor de servicios de certificación

Tanto la doctrina española como el derecho comparado apuntan diversas terminologías para designar al proveedor de s ervicios de certificación, conocido también como prestador de s ervicios de

---

reduciendo los costes de procesamiento y aportando servicios asociados de manera centralizada – por ejemplo, sistemas de liquidación y compensación en los mercados bursátiles -.Fácil es deducir que es ésta una función determinante de las plataformas electrónicas de contratación o *e-marketplaces"*; y *d) Matching.* Localizar el vendedor adecuado a las preferencias del consumidor y encontrar los clientes objetivos dada la oferta del vendedor, aporta un enorme valor añadido. Los buscadores y los *shopbots* son ejemplos paradigmáticos en el desempeño de esta función de *matching",* RODRÍGUEZ DE LAS HERAS BALLELL, T. «Intermediación en la red y responsabilidad civil. Sobre la aplicación de las reglas generales de la responsabilidad a las actividades de intermediación en la Red», en *Revista Española de Seguros,* núm. 142, 2010, pp. 217-259, especialmente p. 237 y ss.

[150] Ibídem, *op., cit.,* p. 25; vid. RODRÍGUEZ DE LAS HERAS BALLELL, T. «Intermediación en la…»op., cit., p. 228.

[151] Vid. GARROTE FERNANDEZ-DIEZ, I.: «La responsabilidad civil extracontractual de los prestadores de servicios en l ínea por infracciones de l os derechos de aut or y conexo*», Revista de Propiedad Intelectual*, nº. 6, 2000, p. 43.

certificación[152], entidades de certificación[153], autoridades de certificación o tercera parte de confianza[154].

Así, el legislador español utiliza la terminología de prestador de servicios de certificación al establecer en el art. 2 apartado 2 de la LFE que: «Se denomina prestador de servicios de certificación a la persona física o jurídica que expide certificados electrónicos o presta servicios a otros servicios en relación con la firma electrónica»[155]. Y en este mismo sentido, el legislador

[152] Este es la terminología utilizada por el grupo de trabajo de la CNUDMI, en la cual el art. 2 e) establece que por prestador de servicios de certificación «se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas».

[153] Portugal: Decreto-Lei n.º 88/2009, sobre Documentos Electrónicos y Actos Jurídicos, de 9 de Abril, que modifica el Decreto-Ley núm. 290-D/99, de 2 de agosto, sobre régimen jurídico de los documentos electrónicos y de la firma digita, en su art. 5, inciso o) define la entidad de certificación como entidad o persona física o entidad que crea o proporciona los medios para crear verificación de firmas, expedición de certificados, asegura su publicidad y presta otros servicios relacionados con firmas electrónicas. Publicado en *Diário da República,* 1. ª série N.º 70 9 de A bril de 2 009. [En línea] disponible en Internet: http://www.uaipit.com/multilingue/documentos.jsp?len=es (última consulta el 12 de enero de 2009).

[154] En la doctrina, ILLESCAS ORTIZ señala que la tercera parte de confianza(Trusted Third Party, TTP) puede ser tanto el prestador de servicios de certificación, como cualquier entidad encargada de un registro de anotaciones en la cuenta de acuerdo con ley de mercado de valores, en ILLESCAS ORTIZ, R.: *Derecho de la contratación...op., cit.,* p. 336; por su parte, en el Derecho Anglosajón se utiliza la terminología Certification Authority; La ley de Utah define a las Autoridades Certificación (CERTIFICATION AUTHORITIES, CA), «como las personas facultadas para emitir certificados. Ya sean personas físicas o empresas o instituciones públicas o privadas y deberán obtener una licencia de la División of Corporations and Commercial Code, en el caso del Estado de Utah, para funcionar como tales. Son las encargadas de mantener los registros directamente en línea "on-line" de claves públicas. Una compañía puede emitir certificados a sus empleados, una universidad a sus estudiantes, una ciudad a s us ciudadanos. Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser confiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que certifique la validez de su clave. Esta solución da origen a diferentes niveles, estratos o jerarquías de CA»; vid. Art. 25 LSSICE, en relación al tercer de confianza; vid. RODRÍGUEZ DE LAS HERAS BALLELL, T, «El tercero de confianza en el suministro de información. Propuesta de un modelo contractual para la sociedad de la información», en *Anuario de Derecho Civil,* Tomo LXIII, Fascículo III, 2010, pp. 1245-1284, especialmente, pp. 1263 y ss; vid. RODRÍGUEZ DE LAS HERAS BALLELL, T.; y ALBA FERNANDEZ, Manuel. «Las agencias de rating como terceros de confianza: responsabilidad civil extracontractual y protección de la seguridad del tráfico», en *RDBB*, núm. 120, octubre-septiembre, 2010, pp.141-177, especialmente, pp. 146 y ss. Esta misma autora, pone como ejemplo de terceros de confianza que suministran información que en muchas ocasiones genera confianza específica en decisiones económicas son las agencias de *rating*.

[155] ESPAÑA: La Ley 59/2003, de firma electrónica.

usaba esa terminología en el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica(RDLFE), derogado, en el que se definía en su art. 2.k que el prestador de servicios de certificación (PSC) «es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica»[156]; el prestador de servicios constituye la tercera parte de confianza que participa en una transacción electrónica.

Por su parte, la Directiva 1999/93/CE define como "proveedor de servicios de certificación", según su art. 2.11, a «la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica».

Como se puede observar, el legislador comunitario prefiere utilizar la terminología "proveedores de servicios de certificación". Es decir, se trata de una entidad pública o privada independiente que, una vez realizadas las comprobaciones pertinentes, asegura que el titular de una firma electrónica es quien dice ser.

Por su parte, el art.2 e) LMFE define al prestador de servicios de certificación como « la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas».

Por último, teniendo en cuenta las distintas terminologías que emplean algunas legislaciones y sectores de la doctrina para referirse a la figura del sujeto que expide certificados electrónicos, creemos que la más adecuada a nuestro estudio es la de prestador de servicios de certificación(tercera parte de confianza), que desempeña función de un intermediario entre consumidor

[156] ESPAÑA. El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, en *BOE,* núm. 224, de 18 de septiembre de 1999); La potestad de emitir estos certificados *SET* en España, lo tiene la Agencia de Certificación Electrónica (AEC), http://www.aec.es. (última consulta 23/11/2009); vid. ILLESCAS ORTIZ, R.: *Derecho de la contratación...op., cit.,* p. 138.

y proveedor de bienes o servicios con la finalidad de garantizar la emisión del mensaje y la identidad de las partes intervinientes en la operativa de pago mediante el uso del número de la tarjeta en el comercio electrónico, especialmente en Internet.

En este mismo sentido, siguiendo el criterio de algunos autores, diremos que "se trata de un tercero que intermedia en la comunicación certificando claves, validando fechas, hora y lugar, y encriptando el documento electrónico con sus claves privadas para luego enviarlo a las partes, quienes desencriptarán con clave pública, posibilitando la prueba de la notificación, autoría, no repudio, autenticación, integridad, etc."[157].

Suscribiendo textualmente la tesis sostenida por algún autor[158], tras sostener que, "la función del tercero de confianza es emitir señal al mercado sobre la fiabilidad, confiabilidad, la exactitud de aspectos relativos al prestador. De este modo, a pesar de la generalizada denominación de esta figura como tercero de confianza, la estructura relacional nos indica, sin embargo, que es en realidad, un «segundo de confianza» con respecto al prestador, habitualmente parte contratante, y un verdadero tercero en el marco de la relación, no siempre contractual, entre el prestador y el usuario o tercero".

Finalmente, se ha de resaltar que lo cierto es que no se puede confundir la función del prestador de servicios (tercera parte de confianza) con la que realizan los notarios y los jueces ya que para ser notario se debe ser jurista y funcionario público; sin embargo, los prestadores de servicios de certificación (tercero de confianza) no cumplen con estos requisitos.

[157] MARTÍNEZ NADAL, A. *Comercio electrónico*…op., cit., p. 32.

[158] RODRÍGUEZ DE LAS HERAS BALLELL, T, «El tercero de confianza en el suministro de información. Propuesta de un modelo contractual para la sociedad de la información», en *Anuario de Derecho Civil,* tomo LXIII, Fascículo III, 2010, pp. 1245-1284, especialmente, pp. 1263 y ss.

En relación al pago con tarjeta en el comercio electrónico, especialmente en Internet, nos interesa resaltar que no suele haber firma electrónica. Por lo que, la intervención de estos intermediarios resulta necesariamente limitada. Ya que, la gestión de los pagos recae en la entidad emisora y gestora de la tarjeta, quien proporciona el software de procesamiento de pagos (pasarela de pagos)[159].

Una vez definido en qué consiste la tarjeta de pago, su clasificación y los sujetos intervinientes en la operativa de pago en el comercio electrónico, es preciso pasar a analizar las distintas operativas de pago mediante tarjeta de crédito o débito existentes en la actualidad.

1.8. Las operativas de pago mediante tarjeta de crédito

En la actualidad existen dos formas de pago con tarjeta de crédito o débito:

- ✓ *Pagos presenciales*: son aquellas operaciones en la que el usuario o titular de la tarjeta la presenta físicamente, ya sea mediante la retirada del efectivo en un cajero automático[160] o en la compra de bienes o servicios en un establecimiento comercial adherido al sistema.

- ✓ *Pagos no presenciales:* son aquellas operaciones realizadas sin la presencia física de la tarjeta, como por ejemplo, las operaciones de

[159] Vid. RODRÍGUEZ DE LAS HERAS BALLELL, T. "Reparto de riesgo…"*op., cit*., pp. 338-341.

[160] El cajero automático o ATM (conocida en Inglés Automated Teller Machine): es una máquina expendedora o un dispositivo externo a través del cual el cliente puede realizar la operación bancaria utilizando la tarjeta de pago (crédito o débito), sin personarse en la caja. Existen dos tipos de cajeros en la actualidad: a) los cajeros automáticos Full: son aquellos que permiten al cliente extraer dinero y a su vez realizar depósitos (mediante un sobre o sin sobre). Estos cajeros suelen estar en el interior del banco; b) los cajeros automáticos Cash no permiten la opción de depósito y suelen ser cajeros secundarios en sucursales (acompañados por un Full) o lo que se llama Cajero extrabancario, como los que se pueden ver en Supermercados, estaciones de servicio, etc.

pagos a través de Internet o el pago de bienes o servicios por vía telefónica.

Teniendo en cuenta el objetivo de nuestra investigación, se ha de destacar la necesidad de estudiar la operativa de pagos no presenciales, principalmente el pago a través de comercio electrónico, especialmente en Internet.

1.9. Marco jurídico de los medios de pago electrónico

Hemos de comenzar señalando que no existe una normativa jurídica específica que regule los aspectos contractuales sobre los medios de pago electrónicos, por lo que para aceptar la utilización de estos medios de pago o instrumentos de pago, habría que recurrir a las normas del derecho civil y mercantil[161], así como a las disposiciones adoptadas en el marco de la Unión Europea[162] sin dejar de lado las condiciones generales establecidas

[161] En cuanto al Derecho español, cabe reseñar diversas normativas que son aplicables a las tarjetas de crédito: la Ley 16/2009, de 13 de noviembre, de Servicios de Pago, transpone al ordenamiento interno la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, de servicios de pago en el mercado interior. (Publicado en el *BOE.,* núm. 275, de 14 de noviembre de 2009); la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero (MRSF). (Publicado, en el *BOE*, núm. 281, de 23 de noviembre de 2001); La Ley 7/ 1995, de 23 de marzo, de Crédito al Consumo, que sólo será aplicable al pago electrónico (Publicado en el *BOE*, núm. 72, de 25 de marzo de 1995); Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista (LOCM)(Publicado, en el *BOE,* núm. 15, de 17 de enero de 1996.), modificada por la Ley 55/1999, de 29 de diciembre, de medidas fiscales, administrativas y del orden social, y por la Ley 47/2002, de 28 de diciembre, para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE, del Parlamento Europeo y del Consejo de 20 de mayo de 1997 en materia de contratos a distancia, y para la adaptación de la Ley a diversas Directivas comunitarias. Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación; El Real Decreto Ley 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, que actualiza la Ley 26/1984, de 9 de julio, (LGDCU) (Publicado en el *BOE*, núm. 287 de 30 de noviembre de 2007).

[162] Entre las disposiciones comunitarias se encuentran las siguientes: Comunicación de la Comisión al Consejo: «Una nueva baza para Europa: las tarjetas de pago electrónico», de 12 de enero de 1987; Recomendación sobre «Código de buena conducta en materia de pago Electrónico» (relaciones entre organismos financieros, comerciantes-prestadores de servicios y consumidores, de 8 de diciembre (87/598/CEE). Publicado en el *DOCE.* L 365 de 24 de diciembre de 1987; la Recomendación, "relativa a los Sistemas de Pago y en particular a las relaciones entre titular y emisor de tarjetas", de 17 de noviembre

unilateralmente por las entidades bancarias, a l as que se adhieren los titulares[163].

A raíz de esta situación, el legislador español promulga la Ley 16/2009, de 13 d e noviembre, de servicios de pag o, por la que se van a r egir los medios de pagos más utilizados por los consumidores (tarjetas de crédito y débito, entre otros instrumentos de pago), con el fin de rellenar una laguna legislativa en cuanto a los instrumentos de pago electrónico.

(88/590/CEE). Publicada en el *DO* L 317, de 24 de noviembre de 1988; La Recomendación 97/489/CEE, es la que actualiza la Recomendación 88/590/CEE. Se aplica tanto a la transferencia de fondo y las retiradas de efectivo mediante instrumento electrónico de pago; La Directiva 97/5/ CE. Publicada en el *DOCE* L 275, el 14 de febrero del 1997 octubre de 2000, pp. 27-28; La Directiva 97/7/ CE. Publicada en el *DOCE,* 4 de junio de 19997; La Directiva: 2000/46/CE. Publicada en el *DOCE,* núm. L 275; La Directiva: 2000/46/CE. Publicada en el *DOCE,* núm. L 275/39, de 27 de octubre de 2000. [En Línea] Disponible en internet: http://www.europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0046.html.(última consulta 2 de diciembre de 2012); La Directiva 1999/93/CE. Publicada en el *DOCE* L 13, de 19 de enero de 2000, el objetivo de esta directiva es mejorar los servicios de transferencia transfronterizas, ayudando al Instituto Monetario Europeo en su tarea de promover la eficacia de las transferencias transfronterizas; La Directiva 2007/64/CE. Publicada en el *DOUE,* L 319, 5/12/2007.

[163] Véanse LAFUENTE SÁNCHEZ, Raúl. *Los servicios financiero…op., cit,* pp. 216 y ss; en este mismo sentido BARRIUSO RUIZ, Señala que además de l as normas de banc a electrónica y banca en casa, la principal fuente de derecho de obligación se constituye por vía racionada y convencional (art.1.255 C. civil.) a través del contrato que se suscribe entre las partes. a la entrega de l a tarjeta electrónica, en BARRIUSO RUIZ, Carlos. *La contratación electrónica* Madrid: Dykinson, 1998, p. 276; GETE-ALONSO Y CALERA. M. C. *El pago mediante tarjetas de crédito*. Madrid: Editorial La ley, 1990, pp. 9 y ss; GÓMEZ MENDOZA, M. «Naturaleza de las tarjetas de crédito, sus clases y carga de la prueba en el supuesto de extradiciones en c ajeros automáticos», en *Revista de Derecho Bancario y Bursátil,* núm. 54, abril-junio, 1999*;* GÓMEZ MENDOZA, M. «Tarjetas de c rédito al consumo» *La ley*, 1993, pp. 789 y ss*;* MARTÍNEZ NADAL, A. «Medios de pago…»*op., cit*., pp.1 y ss; PLAZA PENADÉS, J. « El pago a través de Rede de Comunicación en el Derecho Español y Comunitario», *REDI,* núm. 23, junio 2000; PÉREZ-SERRABONA GONZÁLEZ, J. Luis y FERNÁNDEZ FERNÁNDEZ, Luis. Miguel. *La tarjeta de crédito*. *Derecho comunitario europeo. Doctrina y formulario.* Granada: Comares, 1993, p. 107; BARUTEL MANAUT, Carles. *Las tarjetas de…op., cit.,* pp. 167-168; BERNAL JURADO, Enrique. *El mercado español de…op., cit.,* p. 60; CARRASCOSA LÓPEZ, V.; POZO ARRANZ, Mª. A.; y RODRÍGUEZ DE CASTRO, E. P: *La contratación…*op., cit., p. 42; RAMOS HERRANZ, I.: "Medios de…"*op., cit.,* pp. 542 y ss.

1.9.1. Análisis de la Ley 16/2009, de 13 de noviembre, de servicios de pago (LSP)

Nos parece conveniente que antes de iniciar el estudio de algunos preceptos de la Ley de servicios de pago (LSP)[164] dejemos señalados, aunque fuese brevemente, aquellos aspectos más importantes de dicha normativa por haber sido un primer esfuerzo legislativo eficaz para resolver ciertas cuestiones relacionadas con los servicios de pago.

1.9.2. Ámbito de aplicación de la LSP

El título I de la Ley de servicios de pago contiene las disposiciones generales que regulan los aspectos fundamentales de esta normativa. Es de destacar que en el art.1.2 LSP se delimita el ámbito de aplicación de esta Ley enumerando los servicios de pago a los que se aplica esta norma, en particular.

« a) los servicios que permiten el ingreso de efectivo en una cuenta de pago y todas las operaciones necesarias para la gestión de la propia cuenta de pago; (…).

c) la ejecución de operaciones de pago, incluida la transferencia de fondos, a través de una cuenta de pago en el proveedor de servicios de pago del usuario u otro proveedor de servicios de pago: ejecución de operaciones de pago mediante tarjeta de pago o dispositivo similar;

g) la ejecución de operaciones de pago en las que se transmita el consentimiento del ordenante a ejecutar una operación de pago mediante dispositivos de telecomunicación, digitales o informáticos y se realice el pago a través del operador de la red o sistema de telecomunicación o informático, que actúa únicamente como intermediario entre el usuario del servicio de pago y el prestador de bienes y servicios».

[164] Ley 16/2009, de 13 de noviembre de 2009 (*BOE*, núm. 14 de noviembre de 2009).

No obstante lo señalado con anterioridad, cabe resaltar que el art. 3 de la LSP excluye de su ámbito de aplicación un amplio número de servicios de pago entre los que se encuentran:

- «las operaciones de pago efectuadas exclusivamente en efectivo y directamente del ordenante al beneficiario, sin intervención de ningún intermediario.

- los servicios en los que el beneficiario proporciona dinero en efectivo al ordenante como parte de una operación de pago, a instancia expresa del usuario del servicio de pago inmediatamente antes de la ejecución de una operación de pago, mediante pago destinado a la compra de bienes o servicios.

- las operaciones de pago ejecutadas por medio de dispositivos de telecomunicación, digitales o de tecnologías de la información, cuando los bienes o servicios adquiridos se entregan y utilizan mediante dispositivos de telecomunicación, digitales o de tecnologías de la información, siempre y cuando el operador de servicios de telecomunicación, digitales o de tecnologías de la información no actúe únicamente como intermediario entre el usuario del servicio de pago y el proveedor de los bienes y servicios».

1.9. 3. Objeto de la LSP

La LSP, tiene como objeto la incorporación al ordenamiento jurídico interno de la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, de servicios de pago en el mercado interior. Para ello, en su Exposición de Motivos (II), se enuncia que los objetivos específicos (…) de la presente Ley son los siguientes:

En primer lugar, se persigue estimular la competencia entre los mercados nacionales y asegurar igualdad de oportunidades para competir.

En esta línea, se permite la creación de nuevas entidades de pago que, sin perjuicio de que cumplan importantes exigencias y garantías para su funcionamiento, puedan representar una ampliación de los proveedores de servicios de pago.

En segundo lugar, se pretende aumentar la transparencia en el mercado, tanto para los prestadores de los servicios como para los usuarios. Para conseguir este objetivo es preciso establecer normas comunes, como mejor sistema para ofrecer seguridad jurídica, tanto en el ámbito nacional como en el transfronterizo, toda vez que son uniformes las condiciones y los requisitos de información aplicables a los servicios de pago[165].

En tercer lugar, se establece un sistema común de derechos y obligaciones para proveedores y para usuarios en relación con la prestación y utilización de los servicios de pago. Sin tal ordenación, sería imposible la integración del mercado único de pagos. Todo ello contribuirá a una mayor eficiencia, un nivel más elevado de automatización y un procedimiento común sujeto a legislación comunitaria.

La esencia de esta normativa es adecuar las normas españolas a los consumidores con el fin de crear un marco jurídico común que facilite el funcionamiento del mercado único de los servicios de pago.

1.9.4. Derechos y obligaciones del proveedor y del usuario de servicio de pago

Efectivamente, una de las novedades más destacadas por el legislador español en la LSP es la relacionada con la seguridad de los usuarios en la

[165] Véanse LÓPEZ JIMÉNEZ, José María. *Comentarios a la ley de servicios de pago.* Madrid: BOSH, S.A., 2011, 636 p; GARCÍA RODRÍGUEZ, Ana. «Ley 16/2009, de 13 de noviembre, de servicios de pago: transposición en España del régimen comunitario armonizado», en *RDBB,* núm. 117, enero-marzo 2010, pp. 277 y ss.

utilización de los medios de pago (instrumentos de pago). Siguiendo lo establecido en el inciso a) del art. 28 de la LSP, el proveedor de servicios de pago (emisor de un instrumento de pago) debe «cerciorarse que los elementos de seguridad personalizados del instrumento de pago sólo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento. En particular soportarán los riesgos que puedan derivarse del envío al ordenante tanto de un instrumento de pago como de cualquier elemento de seguridad personalizado del mismo».

Por otro lado, la ley prohíbe a los proveedores de servicios de pago (entidades emisoras) el envío de los medios de pago no solicitados por el usuario, salvo en caso de que deba sustituirse un instrumento de pago y entregarse al usuario de servicios de pago (art.28, b) LSP).

A su vez, la ley exige a los proveedores de servicios de pago que se garantice en todo momento la disponibilidad de medios adecuados y gratuitos que permitan al usuario de un instrumento de pago efectuar la comunicación en caso de extravío, sustracción o utilización no autorizada del instrumento de pago. Además, el proveedor de servicios de pago facilitará gratuitamente al usuario de dichos servicios medios que permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma (art. 28, c) LSP).

Otras de las novedades introducidas por la LSP es la relacionada con el límite de responsabilidad del usuario por uso fraudulento de instrumentos de pago, quedando fijada de la siguiente manera: el ordenante sólo soportará, hasta un máximo de 150 euros, las pérdidas derivadas de operaciones de

pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado o sustraído[166].

A lo largo de este trabajo podrán observar que la aplicación de dicho límite estaba sólo recogida en las diversas recomendaciones de la Comisión Europea, por lo que algunas entidades no lo incluían en sus contratos y otras lo hacían, pero con restricciones. Es decir, no era de carácter vinculante la aplicación del mencionado límite. Asimismo, la ley contempla lo relacionado con la aplicación del límite de responsabilidad a todos los instrumentos de pago, incluyendo aquellas operaciones llevadas a cabo con libretas en un cajero automático, hasta ahora excluidas.

No obstante, es necesario precisar que en la Ley de servicio pago existen inconvenientes como, por ejemplo, cuestiones relacionadas con los comerciantes, según las cuales éstos podrán cobrar suplementos o hacer descuentos por utilizar determinado medio de pago, una práctica que hasta ahora impedían los contratos entre emisores de tarjetas y comercios. A este respecto, encontramos opiniones doctrinales que se oponen a dicho planteamiento, tras considerarlo una medida (...) discriminatoria para determinados medios de pago (por ejemplo, si se cobra más por pagar con tarjeta)[167].

Antes de realizar el análisis sobre las medidas de seguridad en las transacciones electrónicas efectuadas mediante el uso del número de tarjeta de crédito o débito, nos parece imprescindible desarrollar en este primer capítulo un epígrafe sobre ventajas y riesgos en la utilización de la tarjeta

[166] Sobre este aspecto véanse el comentario realizado por GARCÍA RODRÍGUEZ, A. «Ley 16/2009, de…*op., cit.,* pp. 277 y ss.

[167] Organización de Consumidores y Usuarios [En Línea] disponible en internet: http://www.ocu.org/compras-de-productos/nueva-ley-de-servicios-de-pago-s472314.htm (última consulta 2 de diciembre de 20 12); vid. [En Línea] disponible en internet: http://www.consumer.es/web/es/economia_domestica/finanzas/2010/03/03/191476.php (última consulta, 2 de diciembre de 2012).

como medio de pago en Internet, así como los tipos de fraudes en medios de pago electrónico.

1.10. Ventajas en la utilización de tarjeta como medio pago en el comercio electrónico a través de Internet

Como veníamos señalando en los epígrafes anteriores, las tarjetas tradicionales de crédito y débito se han convertido en medios habituales de pago electrónico, utilizando, a efectos de seguridad, protocolos de comunicaciones ya existentes (SSL) o desarrollando otros destinados específicamente al comercio electrónico y a la fase de pago (SET y 3D Secure).

Se ha de resaltar que el uso de la tarjeta de crédito como medio de pago electrónico representa una gran ventaja para los sujetos que intervienen en la operativa de pago en el comercio electrónico a través de Internet. Para el titular, la comodidad en el pago, la facilidad de uso o la seguridad en las transacciones. Para el proveedor de bienes o servicios adheridos al sistema, la seguridad en el cobro y el incremento de ventas que el uso de este instrumento representa; y por último para las entidades emisoras de tarjeta, la captación de clientes a través de este servicio y la percepción de ingresos, tanto por cuotas de titulares como por comisiones de los proveedores de bienes o servicios adheridos al sistema.

1.11. Riesgos en la operativa de pago mediante tarjeta de crédito en el comercio electrónico

No obstante lo señalado en el epígrafe anterior, el pago electrónico mediante el uso de la tarjeta de crédito o débito presenta diversos inconvenientes o riesgos que pueden derivar en algún tipo de fraude[168].

Con el avance de la sociedad de la información y el comercio electrónico, han ido surgiendo numerosos tipos de fraude en relación con medios de pago electrónico. Por lo que la proliferación de los mismos puede repercutir negativamente en la confianza que tienen depositada los consumidores y usuarios en los sistemas de pago electrónico y así convertirse en uno de los principales obstáculos para el desarrollo del comercio electrónico[169].

[168] Según el diccionario de la Real Academia Española, el fraude se define como la "acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete". Es decir, para poder considerar una acción como fraude, este debe ser contraria a la verdad, por lo tanto engañosa, y que suponga un perjuicio contra quien se comete; MARTÍNEZ NADAL. A. *El dinero…, op., cit.,* p. 25; según señala MARTÍNEZ GONZÁLEZ "los riesgos pueden variar de un medio de pago a otro, también puede darse en función de soporte tecnológico o soluciones tecnológico utilizada en su gravedad; y que los riesgos más común en los pagos electrónicos proviene del hecho en que una persona malintencionado suplante alguno de los participantes en una transacción y de los datos confidenciales accesibles a estafadores por falta o mala protección del sistema que almacena los datos o canal de comunicación utilizada durante la transacción. Y este autor señala que los riesgos pueden ser: -Suplantación del comprador (se suplanta para hacer pago con tarjeta o cuenta bancaria de la que no es el titular); -Suplantación del vendedor o servidor de pago (en este caso el estafador hace pasa por el vendedor para con el motivo de obtener los datos confidenciales sobre tarjeta o cuenta del cliente, con la intención de utilizarla en una compara fraudulenta. Esto se da en aquellos servidores web falsos que tiene la misma apariencia con comercio en la que el cliente quiere comprar;-Los datos almacenados en servidores poco segura (se da en aquellos casos en el que el cliente proporciona al vendedor sus datos y este lo almacena en su ordenador temporalmente para tramitar el pago con la entidad bancaria; y -Escucha e intrusiones en la comunicación entre cliente y vendedor. En este caso el riesgo es que un presunto estafador pueda «escuchar» la comunicación entre cliente y proveedor en el momento que se intercambian los datos confidenciales (por ejemplo, los datos de una tarjeta de crédito)…." Y a continuación sostiene este mismo autor, de que todo este riesgo se puede prevenir si los medios de pago electrónicos cumplen con ciertos requisitos por ejemplo: autenticación, confidencialidad, y no repudio", MARTÍNEZ GONZÁLEZ, Mercedes. "Mecanismo de seguridad en el pago electrónico", en M. MATA Y MARTIN, Ricardo (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, pp. 6 y ss.

[169] ADICAE...*op., cit*., p.10.

La inseguridad y la falta de privacidad vienen siendo uno de los principales problemas que plantea el uso de las tarjetas de crédito o débito como medios de pago en el comercio electrónico a través de Internet. Existe la posibilidad de que los datos enviados puedan ser interceptados o rastreados[170] por un tercero ajeno a la comunicación, lo que representa un alto grado de inseguridad en las transacciones electrónicas.

Además, la falta o defectuosa prestación de servicios viene siendo otro de los riesgos que se pueden encontrar en el uso de la tarjeta electrónica. Estos riesgos surgen a raíz del incorrecto funcionamiento de los sistemas informáticos puestos a disposición del titular de la tarjeta o, simplemente, por la falta de interoperabilidad entre los sistemas utilizados por las operaciones en los distintos puntos.

Para algún autor, "…los medios de pagos electrónicos pueden presentar los mismos inconvenientes que los medios de pago tradicionales, ya que el dinero puede ser falso o las tarjetas falsificadas, también existen otros riesgos adicionales que se derivan de la naturaleza: a diferencia del papel, los documentos electrónicos pueden ser copiados sin que se puedan distinguir la copias y el original; también las firmas digitales, técnicas que son aplicadas con frecuencia en estos instrumentos, pueden ser creadas por cualquier sujeto que no sea su titular, que tenga acceso a su clave privada; no se preserva el anonimato del comprador ya que su nombre puede asociarse a los pagos que se realice"[171].

Por último, es de resaltar que la ausencia de los mecanismos de verificación de la autenticidad de la operación existente en el pago con

[170] En este caso adherimos al criterio de FONT Andrés, en la que este señala que uno de los inconvenientes que lleva aparejado la utilización de tarjetas de crédito como medio de pago es que compromete la privacidad de su titular, al permitir que, sus transacciones pueden ser rastreadas, en FONT Andrés. *Seguridad y certificación. En el comercio electrónico.* Madrid: Fundación Retevisión, 2000, pp.139 y 142.

[171] MARTÍNEZ NADAL. A. *El dinero electrónico*. pp. 25 y ss.

tarjeta en las operaciones presenciales a cargo de los proveedores y emisores aumenta el riesgo del uso fraudulento de la tarjeta en Internet[172].

1.12. Tipos de fraudes en medios de pago electrónicos

En la actualidad existen diversos tipos de técnicas para perpetrar fraudes en el comercio electrónico, sobre todo cuando se realizan operaciones de pago mediante el uso del número de la tarjeta en las tiendas virtuales. En este sentido, los tipos de fraudes más frecuentes son: *phishing, código malicioso, pharming, vishing[173], Carta nigeriana[174], spoofing[175], smishing, scam[176], spam,* etc.

[172] Como señala MARIÑO LÓPEZ, que existe un doble riesgo: por un lado, de apropiación por terceros de los datos identificatorios necesarios para realizar pagos por medio de tarjeta de crédito ante la inseguridad de la transmisión de datos en la red abierta de internet y, por otro la utilización ilegitima de la tarjeta ante la ausencia de mecanismos de verificación en la contratación a distancia por medios electrónicos, telefónicos o telemáticos, en MARIÑO LÓPEZ, A. *Responsabilidad contractual…op., cit., p.212 y ss.*

[173] El vocablo *Vishing* es un tipo de fraude con características muy similares al *phishing,* pero en vez de enviar e-mail se realizan llamadas telefónicas por Internet solicitando los números de las tarjetas de créditos, claves secretas, entre otras.

[174] Las famosas cartas nigerianas son aquellos envíos de correos electrónicos que llegan a nuestros buzones de correos electrónicos, en la que sus remitentes nos informan de que hemos ganado lotería o que nuestro correo electrónico fue seleccionado ganador de un sorteo; también pueden consistir en mensajes como por ejemplo, " soy heredero de una gran fortuna, pero con la situación política en mi país no puedo hacer uso y desfrute de estos bienes por lo que le pido que me facilita tu cuenta para hacer una transacciones a tu nombre.

[175] *Spoofing:* son las diferentes técnicas o métodos que utilizan los ciber-delincuentes (hackers) para la suplantación de identidad generalmente con fines maliciosos, por ejemplo, la suplantación de una tercera persona: su sitio web, su correo electrónico o su identidad electrónica(la IP o clave personal). En la actualidad existen diversos tipos de Spoofing: el IP spoofing, ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

IP Spoofing: suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.

Web Spoofing: se trata de la suplantación de una página web, remitiendo la conexión del usuario a través de una página falsa que se aparenta a una página verdadero, con el objetivo de obtener datos personales de la victima (como sitios web vistas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. El atacante puede modificar cualquier información desde y hacia cualquier servidor que la víctima visite. La víctima puede abrir la página web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. Cabe señalar que el sitio web Spoofing es

Entre los tipos de fraudes mencionados con anterioridad, nos limitaremos a analizar solamente aquellos que afectan de forma más directa al pago con tarjeta (*phishing, pharming y código malicioso*)[177].

1.12.1. Phishing

La finalidad de esta técnica fraudulenta consiste en engañar a los usuarios bancarios con el objetivo de apoderarse de sus datos confidenciales, por ejemplo, datos personales, claves de acceso a sus cuentas bancarias por Internet. Para ello, el "*phisher*" o estafador envía cientos de miles de mensajes de texto falsos por medio de correos electrónicos que parecen proceder de la web de la entidad bancaria[178],

---

difícil de detectar, quizá la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente estemos sufriendo este tipo de ataque.

Mail Spoofing: es la suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de e-mails hoax como suplemento perfecto para el uso de phising y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa ip pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales.

DNS Spoofing: suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables.

[176] Para poder comprender en qué consiste el "*Scams*", lo primero que hay que tener en cuenta son las características del phisher y las cartas nigerianas, ya que la unión de estas dos modalidades de fraude en medios de pago da origen a lo que llamamos Scams, que consiste en ofertar trabajos con alta remuneración por chat, foros de discusión, pidiéndoles sus datos personales, número de seguridad social y datos bancarios para así poder contratarlos; vid. ÁLVAREZ MARAÑON, Gonzalo y PÉREZ GARCÍA, Pedro Pablo. *Seguridad informática para empresas y particulares*. Prólogo de Juan Carlos G. Cuartango. Madrid: McGraw-Hill/ Interamericana, S.A., 2004, p. 313.

[177] Vid. ROBLES, Sergi. «Seguridad en redes y protección criptográfica de la información», en *II Congreso sobre las Nuevas Tecnologías y sus repercusiones en el seguro: Internet, Biotecnología y Nanotecnología.* Barcelona, *17 y 18 de noviembre de 2011.* Madrid: SEAIDA, 2012, pp. 77-96, especialmente p. 93.

[178] Según el informe elaborado por INTECO, "este tipo de fraudes tiene lugar a través de la recepción de un correo electrónico con un enlace falso que dirige a una página suplantada de la entidad que supuestamente envía el e-mail", en INTECO. *Estudio sobre el fraude…op., cit.,* p. 53; vid. ROBLES, Sergi. «Seguridad en redes…»*op., cit*., p. 93.

informando al cliente de la necesidad de que confirme información relacionada con su cuenta bancaria, alegando excusas de toda clase. Por ejemplo, modificaciones en el sistema de seguridad, nuevas recomendaciones para la seguridad en las prevenciones de fraude, cambio en las políticas de seguridad de la entidad bancaria, avisos de cancelación de las cuentas si no se procede a la actualización y confirmación de los datos en un corto plazo de tiempo.

Los mensajes enviados por el *phisher* aparecen con el logotipo de la entidad bancaria y demás signos distintivos para aumentar la confusión del usuario. El mensaje contiene un link a un sitio web, que simula ser de la entidad bancaria a la cual pertenece el cliente, pero que en realidad conduce a un sitio web falso. Una vez que el usuario está en el sitio falso, le es requerido que ingrese su información personal sin saber que se transmitirá directamente al estafador quien la utilizará para transferir el dinero a su cuenta, realizar pagos, etc[179].

En este sentido, cabe resaltar que puedan existir hasta cinco tipos de phishing[180]:

a) phishing engañoso, que es el que se realiza mediante chat o e-mail[181].

b) phishing basado en software malicioso, que consiste en la ejecución de software malicioso en el PC de la víctima.

[179] Vid. ÁLVAREZ MARAÑON, Gonzalo y PÉREZ GARCÍA, P. Pa. *Seguridad informática…op., cit.,* p. 310; Belt Ibérica. *Nuevas técnicas de fraude informático: el pharming.* Madrid, 01 de abril de 2005 [En línea] Disponible en Internet: http://www.belt.es/noticias/2005/abril/01/pahrming.htm (última consulta 29 de octubre de 2012); vid. ADICAE. *Catálogo técnico europeo contra el fraude*. Zaragoza: ADICAE, 2009, p. 65.

[180] La clasificación que en el texto se acoge procede de ADICAE *Catálogo…op., cit.,* p. 65.

[181] Por ejemplo, el phishing envía mensajes a los usuarios solicitando contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", entre otras.

c) phishing mediante introducción de contenidos: consiste en introducir contenido malicioso dentro de un sitio web legítimo. Dicho contenido puede tener diversas modalidades: redirigir a los visitantes a otras páginas, instalar algún tipo de *malware* en el ordenador de los usuarios, etc.

d) phishing mediante técnica de intercambio: esta técnica implica el posicionamiento del "*phisher*" entre el ordenador del usuario y el servidor web legítimo. De tal modo el delincuente accede a la información que se transfiere desde el ordenador del usuario atacando al servidor, y viceversa, sin que ninguno de los dos se percate del ataque.

e) phishing de motor de búsqueda: es aquel en el que los delincuentes crean páginas web para la venta de productos o servicios a precios "ganga" y esperan a que los usuarios visiten las páginas para realizar compras y, por tanto, proporcionen información confidencial o directamente realicen transferencias bancarias.

1.12. 2. Pharming

Este tipo de fraude se da sobre todo en ordenadores que están infectados por software malicioso; permite a unos usuarios penetrar en el ordenador de otros usuarios. Una vez que los ciber-delincuentes acceden al ordenador de la víctima manipulan las direcciones DNS (*Domain Name Server)* que utiliza el usuario, de modo que conducen a éste a la página web que desea ver. Pero a través de esta acción, cuando el usuario teclea en su navegador la dirección del sitio web que quiere visitar, en realidad es enviado a otro creado por el estafador, que tiene el mismo aspecto que el original. Así, el usuario introducirá sus datos confidenciales sin darse cuenta de que está remitiendo a un ciber-delincuente.

Además, modifica los mecanismos de resolución de nombres sobre los que el usuario accede a las diferentes páginas web tecleando la dirección en

su navegador. Esta modificación provoca que cuando el usuario introduce en el navegador la dirección del sitio web legítimo, automáticamente es dirigido hacia una página web falsa.

1.12.3. Código malicioso

Este tipo de fraude consiste en aprovecharse de las vulnerabilidades o de los puntos débiles de la seguridad en Internet, con la finalidad de instalar códigos maliciosos para que los usuarios, sin darse cuenta, hagan acciones que permitan que el código se instale o puedan acceder a sus ordenadores[182].

Se señala que cada vez más se utilizan *códigos maliciosos* con el fin de obtener información y beneficios económicos ilícitamente. Este tipo de fraude se ha convertido en el más relevante en la actualidad. Se trata de ataques más complejos técnicamente y difíciles de prevenir, de identificar y de combatir[183].

Según el informe elaborado por INTECO, en septiembre de 2009, un 56,2% de los equipos informáticos estaban infectados con algún tipo de código malicioso; un 35,4% de los equipos alojan troyanos, tipología de malware más relacionada con la comisión de fraude on line[184].

Un *troyano* es una pieza de software dañino disfrazado de software legítimo. No producen efectos realmente visibles o apreciables en el momento de llegar al equipo. Dentro de los troyanos, a su vez, existen diferentes tipos en función de los efectos sobre el sistema. En general presentan un nivel de peligrosidad alta. Entre los tipos de *códigos maliciosos o malware* con un alto potencialidad de riesgo señalaremos: los *troyanos,*

[182] ADICAE. *Catálogo…*op., cit., p. 57.
[183] Vid. INTECO. *Estudio sobre el fraude a través de Internet 2007-2009.*
[184] Ibiden

dialers (marcadores telefónicos), *keyloggers* (registradores de pulsaciones de teclado)[185], *virus, gusanos, rootkits, exploits, y macros.*

Por último, cabe señalar que los diversos tipos de fraudes o técnicas de *Ingeniería Social*[186] examinados a lo largo de este epígrafe no solamente representan una amenaza para los consumidores, sino también para los proveedores de bienes o servicios y las entidades bancarias que operan en Internet ya que la pérdida de la confianza por parte de los consumidores en la seguridad de las transacciones electrónicas pueden repercutir negativamente en dichas entidades.

Por otra parte, cabe resaltar que los tipos de fraudes que hemos mencionado con anterioridad pueden afectar al uso de la tarjeta, por ejemplo copiando u obteniendo los datos personales y bancarios del titular de la tarjeta, etc…

Las entidades bancarias deben establecer las medidas necesarias para que sus sitios webs ofrezcan seguridad en las transacciones. En esta misma línea, se ha de destacar la importancia de los proveedores de acceso a Internet en la lucha contra el fraude en medios de pago, ya que son ellos los que tienen la respuesta inmediata en el bloqueo y análisis de los fraudes electrónicos alojados en sus servidores.

Asimismo, cabe señalar la importancia de los agentes de registro del nombre dominio, ya que mediante el refuerzo de los servicios de registro con medidas de comprobaciones exhaustivas y la rápida respuesta ante la

[185] Keyloggers consiste en capturar y almacenar las pulsaciones efectuadas sobre el teclado. Posteriormente esta información (que puede contener contraseñas, datos bancarios, etc.) se envía a un atacante, que las puede utilizar para fines fraudulentas.

[186] Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos; vid. ROBLES, Sergi. «Seguridad en redes…*op., cit.,* p. 89.

detección de dominios utilizados con fines fraudulentos, aportarán herramientas muy valiosas para evitar que el usuario final se vea afectado por ciertos tipos de fraudes electrónicos.

En definitiva, hemos de resaltar que los tipos de fraude en medios de pago expuesto a lo largo de este epígrafe presentan una serie de efectos jurídicos para los consumidores afectados. En este caso, como señalan algunos sectores de la doctrina, estos tipos de fraude "…afectan a los derechos de intimidad y privacidad establecidos en la constitución y tutelado por distintas leyes, y en ocasiones afectan al funcionamiento de una herramienta del consumidor, como es el caso de sistema operativo que queda inutilizado o no responde con un funcionamiento adecuado. Pero sobre todo, afecta a los derechos económicos de los usuarios"[187].

1.13. Consideraciones finales

Cabe concluir que a lo largo de este capítulo hemos abordado las cuestiones fundamentales del comercio electrónico y los medios de pago electrónicos.

Como hemos podido ver, el riesgo por el uso fraudulento o indebido de la tarjeta se ha venido incrementando cada vez más pero sobre todo en el caso de las transacciones con pago en el comercio electrónico, especialmente a través de Internet. A diferencia de los pagos presenciales, en la operativa del pago por medio de tarjeta de crédito a través de Internet basta que un tercero pretenda usar ilegítimamente la tarjeta que tenga en su poder y los datos de la misma así como los datos de identidad de su titular para poder llevar a cabo el uso fraudulento o indebido. Aunque hay fórmulas adicionales para tratar de identificar al titular.

[187] ADICAE. *Catálogo…* op., cit., p. 57.

Además, la propia operativa de pago mediante el uso del número de la tarjeta y de l os datos de i dentificación del titular o cliente en Internet conlleva el riesgo de que sean interceptados y posteriormente utilizados de forma fraudulenta o indebida en la misma red.

También puede suceder que una vez que el proveedor de bi enes o servicios reciba en un servidor los datos bancarios y los datos de identificación del titular proceda en un futuro a utilizarlas con mala fe.

Universidad Carlos III de Madrid

CAPÍTULO SEGUNDO

SEGURIDAD EN LOS PAGOS MEDIANTE TARJETA DE CRÉDITO O DÉBITO EN EL COMERCIO ELECTRÓNICO

CAPÍTULO II.

Seguridad en los pagos mediante tarjeta de crédito o débito en el comercio electrónico

2. Introducción

Debe destacarse que entre las cuestiones que hay que resolver en el comercio electrónico están las de seguridad e integridad de las comunicaciones, así como la privacidad y protección de los datos personales y bancarios de los consumidores y usuarios, cuando éstos circulan en Internet.

Según se prevé en el punto II de la Exposición de Motivos de la Ley 59/2003, de firma electrónica[188], el desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, (…) el comercio electrónico.

En este sentido, en este capítulo estudiaremos las cuestiones relacionadas con la seguridad en el pago electrónico y los componentes o mecanismos de seguridad exigidos en las operativas de pago electrónico. Además, examinaremos tanto los métodos de la criptografía y la firma digital, como el certificado digital, los protocolos de seguridad necesarios para a

[188] España: La Ley de firma electrónica, 2003.
Ley 59/2003, de 19 de diciembre de 2003, sobre firma electrónica. Publicado en *BOE*, 20 de diciembre de 2003, núm. 304, pp. 1-21, especialmente p.1.

garantizar niveles de seguridad cuando el pago con tarjeta se produce a través de Internet.

2.1. La seguridad en la operativa de pago mediante tarjeta de crédito o débito en el comercio electrónico

La seguridad en el comercio electrónico se ha convertido en una de las mayores preocupaciones para los usuarios y proveedores de bienes o servicios a la hora de realizar transacciones o compras «on-line»[189].Existe sobre todo el temor de los usuarios a proporcionar sus datos (nombre, dirección y número de tarjeta de crédito) a través de Internet para efectuar el pago, ya que pueden ser interceptados por terceros no autorizados y suplantar así su identidad con el fin de utilizarla ilícitamente en su beneficio, lo que representaría un grave riesgo[190]. Además, existe desconfianza por parte de los usuarios en que el pedido cursado y pagado sea realmente entregado[191]. En esta misma línea, como algunos autores apuntan, puede

[189] ALONSO CONDE, A. B. *Comercio electrónico…op., cit.,* pp. 42 y ss; coincidiendo con la tesis de BARRAL VIÑALS, quien sostiene que "uno de los temas más candentes en el comercio electrónico es la seguridad de las transacciones. Y que en realidad, no quiere decir que el entorno sea inseguro, sino que aún no ha sido capaz de generar la suficiente confianza entre los operadores jurídicos", BARRAL VIÑALS, Inmaculada. "La seguridad en Internet: La firma electrónica", en BARRAL VIÑALS, I (coord.). *La regulación del comercio electrónico. Totalmente adaptado a la LSSICE y a la modificación de la Ley del comercio minorista.* Madrid: Dykinson, S.L., 2003, p. 83; ROSSELLÓ MORENO, Rocío. *El comercio electrónico y la protección de los consumidores*. Barcelona: Cedecs Editorial S.L., 2001, pp. 33; transcribiendo textualmente la tesis mantenida por MORENO NAVARRETE, quien sostiene que, "la cuestión de la seguridad jurídica en el comercio electrónico es el tema que más ha preocupado desde su comienzo". Este mismo autor, sostiene que "la falta de presencia física simultanea de los contratantes es una circunstancia que no genera la confianza necesaria en las partes, sobre todo si uno de ellas-consumidor-está en posición teórica desigual respecto la otra", en MORENO NAVARRETE, M. Á. *Derecho-e…op., cit.,* p. 131; Criterio que compartimos, porque la ausencia física de las partes en una transacción como la efectuada en una red abierta como Internet representa un gran obstáculo para el desarrollo del comercio electrónico, sobre todo crea desconfianza en los consumidores a la hora de realizar operaciones en la red; por su parte, TRIAS DE BES sostiene que "la seguridad en el comercio electrónico no es más que un aspecto del principio general de la seguridad jurídica, fundamentado en la base de certeza y legalidad", TRIAS DE BES, X. A. «El pago…», *op., cit.*, pp. 60 y ss.

[190] BARUTEL MANAUT, C. *Las tarjetas…op., cit.,* p. 292.

[191] RIBAS ALEJANDRO, Javier. "Riesgo legales en Internet. Especial referencia a la protección de datos personales", en MATEU DE ROS, Rafael. y CENDOYA MÉNENDEZ DE

ser que el mensaje sea alterado de forma accidental o maliciosa durante la transmisión y también pudiera darse el caso de que el emisor niegue haberlo transmitido o el receptor niegue su recepción[192]; o que la información transmitida sea leída por un tercero no autorizado[193].

Según un estudio realizado por la Asociación Española de Comercio Electrónico (AECE), el principal motivo que hace que los usuarios de internet no realicen sus compras por la vía «on line», es la falta de información, lógica desde la perspectiva de que cualquier novedad necesita un periodo de introducción en el mercado y de modificación de los hábitos de conducta de compra de los consumidores"[194]. A esto se suma la falta de confianza en los medios de pago tanto por parte de los consumidores y usuarios como, de los prestadores de servicios[195].

VIGO, Juan Manuel. (coords). *Derecho de internet. Contratación electrónica y firma digital.* Prólogo de Anna Birules I Bertrán. Navarra: Aranzadi, S.A., 2000, p.147; cabe señalar que la desconfianza de los usuarios sobre la seguridad en el pago con tarjetas de crédito a través de la red de Internet se convierte en unas de las principales barreras para el crecimiento de las transacciones en dicho medio.

[192] MARTÍNEZ NADAL A. *Comercio electrónico...op., cit.,* pp. 31 y ss.; vid. RICO CARRILLO, M. *Comercio…op., cit.,* p.185.

[193] Clasificación técnica de amenazas a la comunicación de datos en sistema de redes Recomendación de la Unión Internacional de Telecomunicación (UIT-X): 800(1991), pp. 32-35;Recomendación UIT-T-X.509 (1993 S), pp. 29-30, citado por MARTÍNEZ NADAL, A. *Comercio electrónico*...op., cit., p. 31.

[194] FERNÁNDEZ GÓMEZ, Eva. *Conocimientos y aplicaciones tecnológicos para la dirección comercial*. Madrid: Editorial ESIC, 2004, p. 207.

[195] Siguiendo a ARIS POU, "la inseguridad que se siente al realizar transacciones electrónicas, por ejemplo, por Internet, deriva de diversas causas como son, entre otras:

- la falta de presencia física simultanea de los contratantes.
- la necesidad de introducir los datos de la tarjeta para realizar el pago por medios electrónicos.
- la incertidumbre de saber si al otro lado de la pantalla estará el prestador de servicios que se anuncia en la página web a través de la que estamos actuando, o se tratará de un impostor...", ARIS POU, María. "Necesidad de seguridad en el comercio electrónico", en *Ciclo de Seminario Europeos contra el fraude en medios de pago. Retos y soluciones para los consumidores en el fraude en medios de pago,* celebrada de 11-12 de mayo. Barcelona. Zaragoza: ADICAE, 2009, p.33; en esta misma línea reafirmándonos, lo antes dicho por ARIS POU, cabe reseñar que la falta de presencia física simultánea de las partes contratantes en las operaciones realizadas mediante el uso del número de la tarjeta en Internet, viene siendo uno de los factores que hace con que los consumidores y usuarios de la tarjeta se desconfían; véanse RODRIGO GONZÁLEZ, sobre las razones que hace con que los

Como hemos indicado en otros apartados de este trabajo en relación a la inseguridad o al riesgo inherente que se presenta cuando se efectúa el pago mediante el uso del número de la tarjeta a través de una red abierta como Internet, y siguiendo la doctrina, diríamos que no sólo es fundamental la seguridad técnica o lógica, sino también la seguridad jurídica[196].

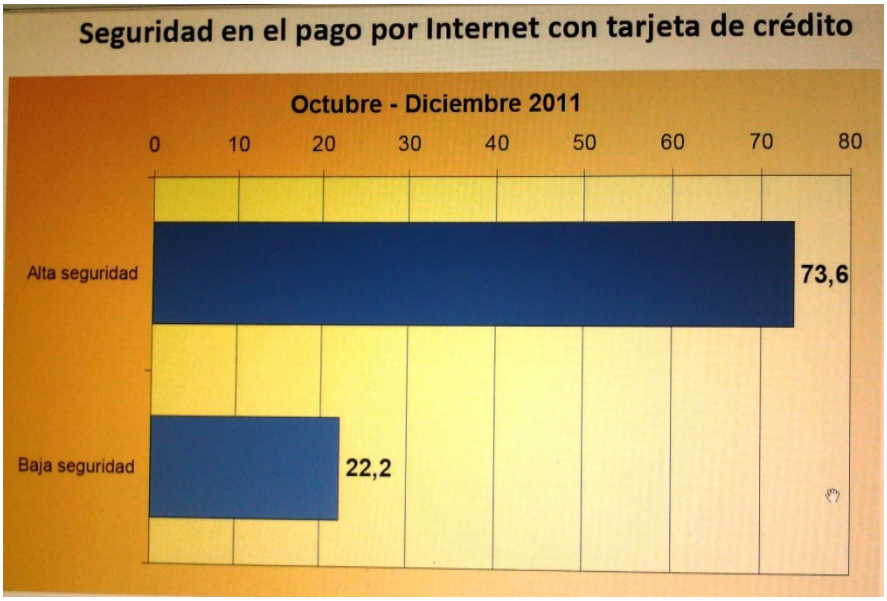
Según el estudio realizado por la AIMC[197], durante los meses de octubre-diciembre de 2011, la confianza en la Red al realizar este tipo de operaciones crece cada año, ya son un 85-90% el número de internautas que han comprado por internet en el último año. Y un 73,6% confían en las tarjetas de crédito para realizar sus pagos por Internet y el 22% no confía. Obsérvese el Grafico 4, a continuación.

consumidores no efectúan compra por Internet. Según éste autor: a) el 35,2% de los usuarios desconfían en las formas de pago; b) un 29% prefieren ver lo que compran; c) el 18,8% tienen miedo a dar datos personales por Internet; d) el 5,6 % desconocen o carecen de informaciones; y e) el 4,8% no se fía en la compra por internet, ya que no le parece segura efectuar la compra por este medio, en RODRIGO GONZÁLEZ, Oscar. *Comercio electrónico*. Madrid: Edit. Anaya Multimedia (Grupo Anaya, S.A.), 2008, pp.166 y ss.

[196] Vid. MARTÍNEZ GONZÁLEZ, M. Mecanismo de seguridad…*op., cit*., p. 7; Normalmente, la estafa por suplantación de identidad empieza con un mensaje de correo electrónico que parece un comunicado oficial de una fuente de confianza, como un banco, una compañía de tarjeta de crédito o un comerciante en línea reconocido. En el mensaje de correo electrónico, se dirige a los destinatarios a un sitio web fraudulento, donde se les pide que proporcionen sus datos personales, como un número de cuenta o una contraseña. Después, esta información se usa para el robo de identidad; véanse ALONSO CONDE, A. B*. Comercio electrónico…op., cit.,* pp. 44 y ss; ROBLES POMPA, J (dir). *Práctica…op., cit.,* pp. 240 y ss; según la tesis sostenida por MADRID PARRA, "la seguridad técnica no es todo. Se puede garantizar la integridad de un mensaje electrónico y su autoría, así como el origen y momento de generación o transmisión del mismo. Pero no es suficiente para alcanzar niveles suficientes de seguridad evidentemente el primero paso ha de ser el desarrollo tecnológico y la puesta a disposición de los medios electrónicos. Pero el paso decisivo para su uso generalizado depende de la confianza que se genere en los posibles usuarios. Dicha confianza descansa no solo en la seguridad que ofrezca la técnica, sino también en la seguridad jurídica", MADRID PARRA, A. "Seguridad en el…", *op., cit.,* p. 124, nota 3; Siguiendo a este planteamiento MORENO NAVARRETE, M. Á. *Derecho-e…*op., cit., p.126; vid. RICO CARRILLO, M. *Comercio electrónico…op., cit*., pp. 186 y ss*.*

[197] AIMC. Publicado 23 de febrero de 2012[En línea] disponible en Internet http://download.aimc.es/aimc/f5g9/macro2011ppt.pdf (última consulta 21 de noviembre de 2012).

Grafico 4



Fuente: AIMC.

La seguridad en las transacciones y operaciones comerciales, tales como la conclusión de contrato o el pago mediante tarjeta (de crédito o débito) realizadas en Internet, se ve afectada fundamentalmente por dos razones:

En primer lugar, las partes contratantes no se encuentran identificadas con total seguridad, es decir, siempre existe la posibilidad que sean diferentes de quienes dicen ser. Esto se debe tanto a la falta de presencia física simultánea de las partes contratantes como a la imposibilidad de verificar la validez del número de tarjeta recibido.

En segundo lugar, los medios de pago tienen una característica particular en este ámbito, es decir, los datos referentes al pago realizado por los consumidores viajan a través de la red Internet. Por ello, existe el temor de que estos datos no sean transmitidos con total seguridad, pudiendo producirse su interceptación para su posterior aprovechamiento ilícito.

Similares consecuencias pueden darse en la transmisión de los datos personales de los consumidores.

Finalmente, se ha de resaltar que la identificación de los sujetos contratantes en el comercio electrónico puede resultar una tarea compleja ya que la falta de presencia física impide conocer con total seguridad con quién se está negociando. Por tal razón, se han creado diversos componentes para lograr reducir la inseguridad reinante en la identificación de los consumidores y proveedores de bienes o servicios en el comercio electrónico.

2.2. Componentes de seguridad exigidos en las transacciones electrónicas

Con el objetivo de dotar de niveles de seguridad a las transacciones electrónicas y a operaciones comerciales tales como la conclusión de contratos o el pago con tarjeta (de crédito o débito) realizadas en Internet, es necesario el cumplimiento de un conjunto de elementos básicos de seguridad que se resumen en[198] "la autenticación, integridad, confidencialidad y el no repudio del origen y destino".

[198] BELTRÁN SÁNCHEZ, Emilio. M. y ORDUÑA MORENO, Javier (dirs.). *Curso de Derecho Privado*. 7. ª ed. Valencia: Tirant lo Blanch, 2004, pp. 246-247; FERNÁNDEZ GÓMEZ, Eva. *Comercio electrónico*. Madrid: McGraw Hill/Interamericana de España S.A.U, 2006, pp.112-113; FERNÁNDEZ GÓMEZ, E. *Conocimientos y aplicaciones...op., cit.,* p. 208; RAMIÓ AGUIRRE, Jorge. «La seguridad informática y sus amenazas», en SOLER MATUTES, Pere (dir.). *Manual de gestión y contratación Informática. Comentarios, jurisprudencia actualizada y formularios de contratos, modelos oficiales del COEIC.* Navarra: Aranzadi, SA., 2006, p.153; VÁZQUEZ RUANO, Trinidad. «La seguridad electrónica en la fase precontractual. Un apunte desde el Derecho comunitario», en MADRID PARRA, A. (dir). *Derecho patrimonial y tecnología.* Madrid: Marcial Pons, 2007, p. 259; RODRÍGUEZ RUIZ DE VILLA, Daniel. *La prestación de los servicios de certificación*, en HUERTA VIESCA, Mª. Isabel y RODRÍGUEZ RUIZ DE VILLA, D.: *Los prestadores de servicios de certificación en la contratación electrónica*. Prólogo de Fernando Sánchez Calero. Navarra: Aranzadi, S.A., 2001, pp. 63 y ss; NORES GONZÁLEZ, Celso. "Marco en el que se desenvuelve la firma electrónica en la Administración General del Estado", en las Jornadas sobre *«Firma digital y Administraciones Públicas»*, celebrada en el Instituto Nacional de Administración Públicas (INAP), de 8 a 9 de junio de 2002. Madrid: INAP, 2003, p. 19.

a) Autenticación

Permite a las partes intervinientes en la transacción (cliente y proveedor de bienes o servicios) asegurarse de que son realmente quienes dicen ser[199] sin que exista la posible equivocación de identidades ni la suplantación por parte de un tercero[200]. De este modo, todos conocen ciertamente la identidad del otro evitando fraudes[201]. Este requisito es un paso importante en el pago electrónico. El cliente necesita estar seguro de que está negociando con quien dice ser para no proporcionar sus datos bancarios a alguien que pudiera utilizarlos de manera fraudulenta[202].

b) Confidencialidad

La confidencialidad evita que la información sea interceptada por un tercero no autorizado. De hecho, tanto el adquirente como la parte emisora no

[199] Véanse, DE MIGUEL ASENSIO, P.A., *Derecho privado…op., cit*., p. 400*;* FERNÁNDEZ GÓMEZ, Eva. *Comercio...op., cit.,* p.113; PLAZA PENADÉS, J. "Contratación*…" op., cit.,* 492 p; MARTÍNEZ NADAL A. *Comercio electrónico…op., cit,* p. 33; RICO CARRILLO. M. *Comercio electrónico…*op., cit. p.187; vid. BIDGODI, Hossein. *Electronic commer. Principle…*op., cit., p. 206.

[200] DE QUINTO ZUMARAGA, Francisco. *La firma electrónica. marco legal y aplicaciones prácticas*. Barcelona: Difusión Jurídica y Temas de Actualidad, S.A., 2004, p. 37; GUIJARRO COLOMA, Luis. "Fundamentos técnicos..."*op., cit.,* p. 233; VASQUEZ CALLAO, Enrique y BERROCAL COMENAREJO, Julio. *Comercio electrónico…op., cit.,* p.17.

[201] En la doctrina FRAMIÑAN SANTAS, señala que "con la utilización de la clave pública unido a la intervención de una autoridad de certificación se pretende de alguna forma lograr que el deudor tenga la certeza, o confiar razonablemente de que aquella persona a la que está enviando la información bancaria para cobrar la deuda es realmente su acreedor, viceversa, que este último también cepa que el titular de la tarjeta es quien dice ser y no una tercera persona. Se desea proporcionar un sistema con el que el titular de la tarjeta no puede negar la utilización de la tarjeta a través de Internet, cuando esta la ha usado. También con la autenticación se pretende evitar que la información sea alterada su transmisión por un tercero", en FRAMIÑAN SANTAS Javier. "Pagos en la red…"*op., cit.,* pp. 378 y ss; MARTÍNEZ GÓNZALEZ, M. "Mecanismo de seguridad…"*op., cit.,* p. 8; ROSSELLÓ MORENO, R. *El comercio electrónico…op., cit.,* p. 24.

[202] GUIJARRO COLOMA, Luis. «Fundamentos técnicos y operativos de la firma electrónica», en SANJUAN y MUÑOZ, E. *Incorporación de las nuevas tecnologías en el comercio: aspectos legales.* Madrid: Consejo General de Poder Judicial, 2006, p.233; RICO CARRILLO, M. *Comercio…op., cit.,* p. 187; BELTRÁN SÁNCHEZ, E. M. y ORDUÑA MORENO, J (dirs). *Curso de Derecho…op., cit*., p. 247*;* BARRAL VIÑALS, I. "La seguridad en…"*op., cit.,* pp. 83 y ss.

pueden conocer los términos del negocio al que se corresponde el pago[203]. La confidencialidad es elemental para el desarrollo del comercio electrónico y para fomentar la confianza entre las partes intervinientes en él, ya que indirectamente se protege el secreto de las comunicaciones[204]. Pues bien, uno de los mecanismos que utiliza el protocolo SET y SSL para garantizar la confidencialidad es el uso de la criptografía para cifrar (encriptar) los datos que se van a enviar[205].

[203] Véanse, FRAMIÑAN SANTAS, J. "Pagos en la red…", *op., cit.,* pp. 378 y ss; según sostiene MARTÍNEZ NADAL, que la confidencialidad y privacidad: "en ocasiones el comprador quiere tener la seguridad de que la transacción es privada, de forma que no pueda ser conocida por terceros y, especialmente, no pueda utilizarse, junto con otras transacciones, para trazar perfiles personales a partir de sus hábitos comerciales. Y que, al mismo tiempo puede desear que ciertas informaciones de la transacciones no sean conocidas por todas las partes que intervienen en la misma (por ej., que el proveedor de bienes o servicios no tenga acceso a los datos de su tarjeta, que solo podrán ser conocidos por el banco. Esta misma autor advierte que a diferencia de la integridad a la autenticación, la confidencialidad de las transacciones no es estrictamente una exigencia jurídica-mercantil. Sin perjuicio de que pueden ser una exigencia comercial, de las partes implicadas, que por razones empresariales no requieren dar publicidad a determinadas…)", en MARTÍNEZ NADAL, A·L. *El dinero electrónico. Aproximación jurídica*. Madrid: Civitas, 2003, p.27; vid. ÁLVAREZ MARAÑON, señala que "la información de pago se cifra para que no pueda ser espiada mientras viaja por las redes de comunicaciones. Solamente el número de tarjeta de crédito es cifrado por SET, de manera que ni siquiera el comerciante llegará a verlo, para prevenir fraudes. Si se quiere cifrar el resto de datos de la compra, como por ejemplo qué artículos se han comprado o a qué dirección deben enviarse, debe recurrirse a un protocolo de nivel inferior como SSL", en ÁLVAREZ MARAÑON, G. *Medios de pago en Internet. op., cit.,* pp. 217-233; MARTÍNEZ GONZÁLEZ, M. *Mecanismo de seguridad, op., cit.,* p. 8; RICO CARRILLO, M. *Comercio electrónico…op., cit*., p.183; GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit.,* p. 233; PLAZA PENADÉS, J. "Contratación electrónica*…"op., cit.,* p. 492; por su parte, el art. 5.1 de la Directiva 97/66/CE establece "los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente, de conformidad con el apartado 1 del artículo 14".

[204] DE ROSSELLÓ MORENO, R. *El comercio electrónico…op., cit*., 26 p ; RAMIÓ AGUIRRE, Jorge. "La seguridad informática..."*op., cit.,* p.153; DE QUINTO ZUMARAGA, Fco. *La firma electrónica...*op., cit., p.36; GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit*., p. 233; ÁLVAREZ MARAÑON, G y PÉREZ GARCÍA, P. P. *Seguridad informática…op., cit.,* pp. 94 y ss.

[205] MARTÍNEZ GÓNZALEZ, M. "Mecanismo de seguridad…" *op., cit*., p. 8.

c) Integridad

Se trata de garantizar que la información intercambiada no sea modificada o alterada ilícitamente durante su envío a través de redes telemáticas[206]. Para lograrlo, se utilizan protocolos de seguridad (SSL, SET y 3D Secure) capaces de detectar cualquier cambio que se haya producido en la información transmitida[207].

d) El no rechazo o no repudio

El no rechazo o no repudio[208]: es aquel servicio que garantiza a las partes intervinientes en una transacción o comunicación que la otra parte ha participado evidentemente en la comunicación, impidiendo el repudio de una transacción (cuando un cliente niega haber realizado la compra o haber enviado un mensaje) y proporcionando a compradores y vendedores la misma

[206] MARTÍNEZ LÓPEZ, Luis; MATA MATA, Francisco y BERNAL JURADO, E. *Medios de pago electrónico. Piedra angular en el desarrollo del comercio electrónico.* [En Línea] disponible en Internet: http://150.214.178.8/sinbad2/files/publicaciones/77.pdf (última consulta 18 de febrero de 2012).

[207] Vid. MARTÍNEZ GÓNZALEZ, M. "Mecanismo de seguridad…", *op., cit.,* p.9; DE ROSSELLÓ MORENO, R. *El comercio electrónico…op., cit.,* p. 25; H. GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit.,* p. 233; SÁNCHEZ, E. M. y ORDUÑA MORENO, J (dirs). *Curso de Derecho…op., cit.,* p. 247. FERNÁNDEZ GÓMEZ, E. *Comercio...op., cit.,* 113*;* RICO CARRILLO, M. *Comercio electrónico…op., cit*., p. 187; RAMIÓ AGUIRRE, J. La seguridad informática... *op., cit.,* p. 153.

[208] Según señala MARTÍNEZ NADAL, "el no repudio implica la autenticación y la integridad de mensaje, y en este caso se consiguen con los efectos de una firma digital. pero no a la inversa, es decir la autenticación y la integridad de un mensaje no implica necesariamente el no rechazo, como en el caso de la criptografía simétrica", en MARTÍNEZ NADAL A. *Comercio electrónico…op., cit.,* pp. 32 y ss; PLAZA PENADÉS, J. "Contratación electrónica…"*op., cit.,* p. 492, nota 14; SÁNCHEZ, E. M. y ORDUÑA MORENO, J (dirs). *Curso de Derecho…op., cit.,* p. 247; ALCOVER GRAU, G. «La firma electrónica como medio de prueba (valoración jurídica de los criptosistemas de claves simétricos)», en *Cuadernos de Derecho y Comercio*, núm. 13, 1994, pp. 11 y ss; ibídem, «El Real Decreto Ley sobre firma electrónica», en *Revista de la Contratación Electrónica*, núm. 1, 2000, pp. 7 a 28; LLANEZA GONZALÉZ, Paloma. *Internet y comunicaciones digitales. Régimen legal de las tecnologías de la información y la comunicación*. Barcelona: Bosch, 2000, p. 296; vid. MARTÍNEZ LÓPEZ, Luis; MATA MATA, Francisco y BERNAL JURADO, Enrique. *Medios de pago electrónico. Piedra angular en el desarrollo del comercio electrónico. [En línea] disponible en Internet:* http://150.214.178.8/sinbad2/files/publicaciones/77.pdf(última consulta 17 de agosto de 2012).

confianza que existe en las compras convencionales usando las actuales redes de autorización de créditos de las compañías de tarjetas de pago. Existen dos tipos de no repudio:

d.1) No repudio de origen. limplica que el emisor del mensaje no niegue haber enviado el mensaje[209].

d.2) No repudio de destino, por el que el receptor no puede negar la recepción del mensaje[210]. Es imprescindible tener la certeza de que el documento o mensaje ha sido efectivamente enviado y recibido por las partes intervinientes y, al mismo tiempo, tener posibilidad de demostrarlo[211]. Si no existe dicha posibilidad cualquiera de las partes podría negar su participación en la transacción y desvincularse de las obligaciones que les corresponden y podrían poner a la otra parte que no la niega en una situación difícil, debiendo tener la prueba de su existencia.

Así, para evitar el repudio del mensaje, el art. 25 de la LSSICE permite la intervención de terceros de confianza que certifiquen la emisión y recepción en la que aparece fecha y hora[212].

[209] MARTÍNEZ NADAL A. *Comercio electrónico…op., cit,* p. 33.

[210] DE ROSSELLÓ MORENO, R. *El comercio electrónico…*op., cit., p. 25; vid. RUIZ-GALLARDÓN, M.: "Fe pública y contratación telemática" en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital.* Prólogo de Anna Birules I Bertrán. Navarra: Aranzadi, S.A., 2000 p.105; SUAREZ RAMOS, Fernando. Eficacia Jurídica de una Transacción Electrónica. La Figura del No Repudio, en la *RDI-alfa redi* [En línea] Disponible en Internet: http://www.alfa-redi.org/rdi-articulo.shtml?x=300 (última consulta 23 de Abril de 2012).

[211] DAVARA RODRÍGUEZ, M. Á. *La seguridad en las transacciones electrónicas: La firma electrónica.* Madrid: Universidad Pontificia Comillas de Madrid, 2005, p. 39; DE ROSSELLÓ MORENO, R. *El comercio electrónico…*op., cit., p. 25.

[212] Según dispone el apartado primero del art 25. LSSICE «Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública. Y en esta misma línea, el apartado segundo de la misma norma prevé lo siguiente" El tercero deberá archivar en

Además de los componentes señalados con anterioridad existen otros requisitos que se usan en el sistema de pago:

-*Intimidad*: el banco emisor de la tarjeta de crédito no puede acceder a la información sobre los pedidos del titular por lo que queda incapacitado para elaborar perfiles de hábitos de compra de sus clientes.

-*Verificación inmediata*: proporciona al comerciante una verificación inmediata, antes de completarse la compra, de la disponibilidad de crédito y de la identidad del cliente. De esta forma, el comerciante puede cumplimentar los pedidos sin riesgo de que posteriormente se invalide la transacción.

Por último, se ha de destacar que los métodos básicos para hacer cumplir las condiciones o componentes de seguridad mencionados con anterioridad son: las técnicas criptográficas (asimétricas o simétricas), la firma digital y los certificados electrónicos. Desempeñan especial importancia en la protección técnica de los datos y constituyen un factor esencial en el desarrollo del comercio electrónico toda vez que garantizan la protección del material sobre la forma digital. Igualmente, estas tecnologías seguras, basadas en métodos criptográficos, promueven la confianza financiera a través de la seguridad de los pagos electrónicos[213].

2.3. El uso de los métodos criptográficos en las transacciones electrónicas

Se ha de resaltar que la criptografía fundamentalmente otorga seguridad a la transacción y no a la operación de pago.

---

soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años»; vid. SÁNCHEZ, E. M. y ORDUÑA MORENO, J (dirs.). *Curso de Derecho…* op., cit., p. 247.

[213] A juicio de DÍAS PEREIRA, en lo esencial, se trata de tecnologías criptográficas que son ampliamente reconocidas como herramientas necesarias para la seguridad y la confianza en la comunicación electrónica. DIAS PEREIRA, A. Liborio. *Comercio electrónico na sociedade da informação: Da segurança técnica a segurança jurídica.* Coímbra (Portugal): Livraria Almedina, 1999, p.19.

2.3.1. Criptografía: concepto y finalidad

El vocablo criptografía que proviene de la lengua griega (κρύπτω krypto, «oculto» y γράφω graphos, «escribir», o sea, literalmente, «escritura oculta»)[214] es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales. Es empleada frecuentemente para permitir un intercambio de mensajes que sólo pueden ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Para hacer un estudio exhaustivo de la criptografía como ciencia es indispensable hablar de la criptología[215] que a su vez abarca tanto las técnicas de cifrado, es decir la criptografía propiamente dicha, como las técnicas complementarias, entre las que se incluye el criptoanálisis que estudia métodos empleados para descifrar[216] textos cifrados con objeto de recuperar la información original en ausencia de las claves.

La criptografía ha sido utilizada desde la antigüedad especialmente con fines militares, políticos o diplomáticos. Así, en el imperio romano, el emperador Julio César utilizaba el sistema criptográfico para comunicarse con los altos mandos militares que se encontraban en el campo de batalla[217]. El algoritmo de César consistía en reemplazar una letra del abecedario por otra, como ejemplo: a por f; b por g; c por x; y así sucesivamente[218]. Sin embargo,

[214] ZAGANI, Raimondo. *Firma digitale e sicureza giuridica*. Casa Editrice Dott. Antonio Milani (CEDAM), 2000, 35 p; vid, el concepto sobre criptografía [En Línea] Disponible en Internet: http://www.es.wikipedia.org/wiki/Criptograf%C3%ADa#Finalidad(última consulta 20 de diciembre de 2010).

[215] Siguiendo lo citado anteriormente en el texto principal diríamos que la criptología, es la ciencia que estudia los distintos sistemas de cifrados destinados a ocultar el significado del mensaje a otras personas que no sea el emisor y receptor de la misma.

[216] El descifrado es el proceso inverso que recupera el texto claro a partir del criptograma y la clave.

[217] FERNÁNDEZ GÓMEZ, E. *Comercio...op., cit.,* pp. 114-115.

[218] GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit.,* p. 236; FERNÁNDEZ GÓMEZ, Eva. *Comercio...op., cit.,* p. 210; MUÑOZ MUÑOZ, Ramiro. "Criptografía", en RUBIO VELÁZQUEZ, Raúl; RODRÍGUEZ SAU, Carlos y MUÑOZ MUÑOZ, R (coords.). *La firma electrónica. Aspectos legales y técnicos*. Barcelona: Ediciones Experiencia, S.L., 2004, 179 p; RICO CARILLO, M*. Comercio electrónico…op., cit.,* p.189*;* COUTO CALVIÑO, Roberto.

con el desarrollo del comercio electrónico el uso de la criptografía ha dado un gran giro hacia la difusión de técnicas criptográficas para fines no bélicos[219].

Como ya hemos indicado, la criptografía[220] es aquel conjunto de técnicas que, mediante la utilización de algoritmos y métodos matemáticos, sirven para cifrar y descifrar mensajes; o sea, no es más que una herramienta para dotar de seguridad a la transmisión y almacenamiento de datos a través de redes informáticas, ya que permite ocultar los datos por medio de su transformación en formato ininteligible (cifrado)[221] y evitar su modificación y uso no autorizado.

De hecho, la finalidad que persigue la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre las partes intervinientes en una transacción on line y, en segundo lugar, asegurar que la información que se

Servicios de certificación de firma electrónica y libre competencia. Prólogo de, Ana Mª Tobio Rivas. Granada: Comares, 2008, p. 33.

[219] MARTÍNEZ NADAL A. *Comercio electrónico…op., cit.,* p. 42; MORENO NAVARRETE, M. A. *Contratos electrónicos*. Madrid: Marcial Pons, 1999, p. 104.

[220] Según se define en el diccionario de la Real Academia Española de la Lengua, que la criptografía es "el arte de escribir con clave secreta o de forma enigmática"; por su parte, el Diccionario Enciclopédico de Tecnología define la criptografía como una "ciencia cuyos métodos permiten cifrar los mensajes antes de su transmisión (mediante diferentes algoritmos que eviten su captación no deseado) y su recuperación en forma inteligible en el lado receptor"*,* en *Diccionario Enciclopédico de Tecnología*. Edición del CL Aniversario de la Ingeniería Industrial. Editor José María Martínez Val-ETS Ingenieros Industriales UPM. Madrid: Editorial Síntesis, 2000, p. 537. citado por DAVARA RODRÍGUEZ, M.: *La seguridad…op., cit*., p. 39; vid. GUIJARRO COLOMA, L. "Fundamentos técnicos...",*op., cit*., pp. 234 y ss; MARIÑO LÓPEZ, A. *R responsabilidad civil*…op., cit., p. 147; por su parte, RAMOS SUAREZ, quien define la criptología como aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Abarca por tanto a la Criptografía (datos, texto, e imágenes), Criptofonía (voz) y al Criptoanálisis (ciencia que estudia los pasos y operaciones orientados a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave), RAMOS SUAREZ, F.: "Firma digital", *RDI*, núm. 009, de abril del 1999. [En línea] Disponible en Internet: http://www.alfa-redi.org/rdi-articulo.shtml?x=252(última consulta 2 de enero de 2012); vid. BIDGODI, Hossein. *Electronic commer. Principles…o., cit*., p. 207; vid. ROBLES, Sergi. «Seguridad en redes…»*op., cit*., p. 85.

[221] El cifrado es el proceso de transformar un texto o mensaje inteligible (en claro), en uno ininteligible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el algoritmo de cifrado para cada uso distinto; vid. RAMIÓ AGUIRRE, J. "La seguridad informática..."op., cit., p. 155; ÁLVAREZ MARAÑON, G.; y PÉREZ GARCÍA, P. P. *Seguridad informática…op., cit.,* p. 151.

envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito. Como señalan algunos autores la criptografía, "es la base de los mecanismos de seguridad que garantizan la confidencialidad de los datos, de la firma digital y de los certificados digitales"[222]. A continuación, estudiaremos, para una mejor comprensión de las cuestiones relativas a nuestro estudio, los dos tipos de sistemas criptográficos existentes: los simétricos o de clave privada y los asimétricos o de clave pública.

2.3.2. Clases de criptografía

2.3.2.1. *Sistema simétrico o de clave privada*

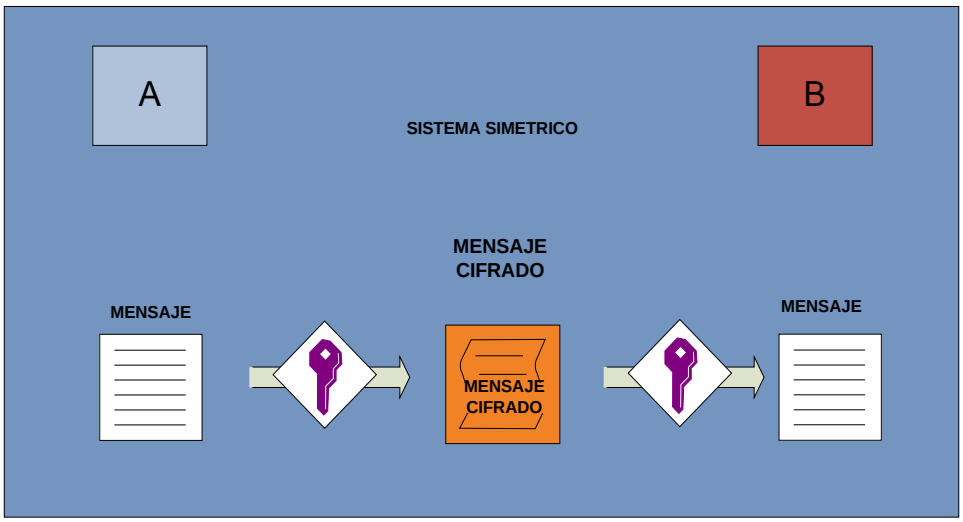
La criptografía simétrica o de clave secreta[223] es una técnica en la que tanto el emisor como el receptor del mensaje operan con el mismo código de encriptación y desencriptación de los mensajes o información, siendo necesario que las partes en comunicación acuerden previamente una clave

[222] MARTÍNEZ GONZÁLEZ, M. "Mecanismo de seguridad…", *op., cit.*, p. 26.

[223] Véanse MARTÍNEZ NADAL A. *Comercio electrónico…op., cit.,* p. 42. RICO CARRILLO, M. *Comercio…op., cit.,* p. 191; ROBLES POMPA, J (dir.). *Práctica y…op., cit.,* p. 241; ALONSO CONDE, A. B. *Comercio electrónico…op., cit*., pp. 31-32; GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit.,* p.235; MARIÑO LÓPEZ, A. *Responsabilidad civil*…op., cit., p. 147; CASTELLANO DE UBOA, Leopoldo González-Echenique. "Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre firma electrónica", en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital.* Prólogo de Ana Birulés I Bertrán Elcano (Navarra): Aranzadi, 2000, pp. 207 y ss; MORENO NAVARRETE, M. A. *Contratos…op., cit.*, p. 106; FONT, A. *Seguridad…op., cit.,* pp. 54 y ss; ZAGANI, R. *Firma digítale…op., cit.,* p, 35; RICO CARRILLO, M. *Firma electrónica*, Conferencia impartida en el Curso del Doctorado en Derecho, programa general. Getafe: Universidad Carlos III de Madrid, 27 de enero de 2006; MATEO HERNÁNDEZ, José Luis. *El Dinero Electrónico en Internet. Aspectos técnicos y jurídicos.* Granada: Comares, 2005, pp, 380 y ss; BRIZ, Julián y LASO, Isidro. *Internet y comercio electrónico. Características, estrategias, desarrollo y aplicaciones.* Madrid: Coedición, ESIC EDITORIAL y Mundi-Prensa, 2000, p. 393; MARTÍNEZ LÓPEZ, Luis; MATA MATA, Francisco y Rodríguez Domínguez, Rosa Mª. Sistemas de pago seguro. Seguridad en el comercio electrónico, en *Revista de Estudios Empresariales*. Segunda época, núm .1, 2009, 67p. [En Línea] Disponible en Internet: http://www.revistaselectronicas.ujaen.es/index.php/REE/article/download/359/322(última consulta 19 de febrero de 2012); ROBLES, S. «Seguridad en redes…», *op., cit.,* p.85.

secreta, con la desventaja de tener que encontrar el modo seguro de cambiar de clave. En efecto, en este tipo de sistema se utiliza una sola clave para cifrar y descifrar los datos. Por ejemplo: la figura 2 muestra el procedimiento del sistema simétrico, en el que el emisor del mensaje (A) cifra utilizando una determinada clave y ,una vez cifrado, lo envía a (B); una vez que éste recibe el mensaje, lo descifra utilizando la misma clave que usó el emisor(A) para cifrarlo.

Figura: 2. Sistema simétrico



Fuente Elaborado por el propio autor

El sistema simétrico[224]proporciona la autenticidad entre las partes ya que solamente la otra parte con la que se comparte la clave secreta puede haber cifrado el mensaje; también proporciona la integridad, ya que si el mensaje ha sido alterado será ininteligible al descifrarlo; en cuanto a la confidencialidad de la información, únicamente las partes implicadas podrán descifrar el mensaje[225]; por último, no garantiza el no rechazo de origen ya que no hace uso de una firma digital. Para que la comunicación sea segura, es necesaria

[224] VÁSQUEZ CALLAO, E y BERROCAL COLMENAREJO, J. *Comercio electrónico...op., cit.,* p.18; FERNÁNDEZ GÓMEZ, E. *Comercio...op., cit.,* p.115; MUÑOZ MUÑOZ, R. "Criptografía", en RUBIO VELÁZQUEZ, R; y RODRÍGUEZ SAU, C.: *La firma electrónica...op., cit.* p.180.

[225] ROBLES POMPA, J (dir.). *Practica y…*op., cit., p. 241; JULIA BARCELÓ, R. *Comercio electrónico...op., cit.,* p. 227.

que la clave sea mantenida en secreto entre las partes involucradas. Así pues, es fundamental la gestión de la distribución y utilización de la clave secreta para evitar que la misma sea modificada en su trayecto.

Este sistema de clave secreta presenta ciertos inconvenientes en relación a la distribución de las claves[226]. No ofrece todos los servicios de seguridad exigida legalmente[227], a pesar de que ofrece la autenticación e integridad entre las dos partes que comparten la clave secreta; sin embargo, no frente a terceros (una tercera parte no podrá determinar con certeza el emisor del mensaje, ni su contenido o la persona que lo ha modificado, porque una de las partes que comparte la clave secreta común podría haberla usado para falsificar el nombre de la otra parte, o podría haber alterado el contenido del mensaje[228]).

Así, el intercambio de la misma clave para cifrar y descifrar los mensajes hace que una tercera persona no pueda determinar cuál de los dos (emisor y receptor) es el autor del mensaje. Teniendo en cuenta los inconvenientes señalados, los sistemas de cifrado simétricos no son aptos para ser utilizados en una red como Internet, en la que confluye una pluralidad indeterminada de entes que no se conocen entre sí y que en la mayoría de los casos no podrán intercambiar previamente claves de cifrado por ningún medio seguro[229].

2.3.2.2. *Sistema asimétrico o de clave pública*

La criptografía asimétrica o de clave pública permite el intercambio de información cifrada sin la necesidad de que los intervinientes compartan una

[226] MARTÍNEZ NADAL A. *Comercio electrónico…op., cit.,* p.43; FONT, A. *Seguridad*…op., cit., pp. 54-55; ZAGANI, R. *Firma digítale…op., cit.,* pp. 40 y ss.

[227] MARTÍNEZ NADAL A. *Comercio electrónico…*op., cit., p 43.

[228] Ibídem*;* RICO CARILLO, M*. Comercio electrónico Internet y Derecho,* 2 ª.ed. Venezuela: Editorial LEGIS, S.A., 2005, p.191.

[229] MUÑOZ MUÑOZ, R. "Criptografía..." *op., cit.,* p.181; JULIA BARCELÓ, R. *Comercio electrónico...op., cit.,* pp. 227 y ss; VEGA VEGA, J. A.. *Contratos electrónicos…o., cit.,* p. 123.

clave secreta común fijada previamente[230]. El uso de dos claves distintas en el sistema asimétrico permite evitar los inconvenientes que presenta el sistema simétrico, ya que se utilizan claves relacionadas matemáticamente para cifrar y descifrar[231]. Se basa en la utilización de dos claves en una única operación criptográfica (clave pública o clave privada) que establecen entre sí una relación compleja; el término del mensaje cifrado por la clave pública sólo puede ser descifrado por la clave privada y viceversa[232].

La clave privada sólo puede ser conocida por su titular que debe mantenerla en secreto. Se utiliza para cifrar mensajes y descifrar el mensaje recibido que se encuentra cifrado[233]. Por su parte, la clave pública puede ser

[230] Vid. ALCOVER GARAU, G. «La firma electrónica...*op., cit.,* pp.11-14; MARIÑO LÓPEZ, A. *Responsabilidad civil*…op., cit., p. 148; El sistema asimétrico más utilizado es el denominado RSA, sigla que corresponde los iniciales de sus fundadores (Ronald Riveste, Adi Shamir y Leonardo Adelman), que en 1978 crearon este sistema; LLANEZA GONZALÉZ, P. *Internet y...op., cit.,* p. 305; BRIZ, J.; y LASO, I. *Internet y comercio...op., cit.,* p.395; ROBLES, S. «Seguridad en redes…», *op., cit.,* p.85.

[231] GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit.,* p. 233; DE MIGUEL ASENSIO, Pedro A. *Derecho Privado de Internet*, 3. ª ed. Madrid: Civita, 2002, pp. 383 y ss; MARIÑO LOPEZ, A. *Responsabilidad civil*…op., cit., p.148; MORENO NAVARRETE, M. A. *Contratos…op., cit.,* p. 105*;* FONT, A. *Seguridad…op., cit.*, p. 55; HERNANDEZ LAVADO, Luis. "Contratación electrónica", en PERALES SANZ, José Luis (dir.). *La seguridad jurídica en las transacciones electrónicas. Seminario organizado por el Consejo General del Notariado en la UIMP*. Madrid: Civitas, 2002, p.153; ZAGANI, R. *Firma digítale…op., cit.,* p. 43*;* LOMASCOLO SZITTYAY, R. *Aspectos técnicos de...op., cit.,* pp. 68 y ss.

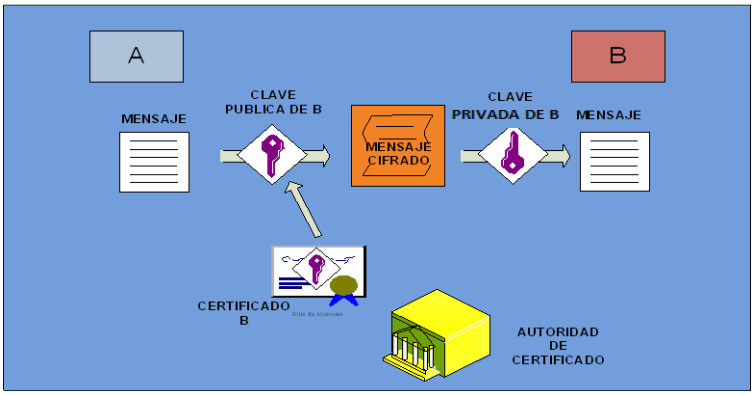
[232] DIAS PEREIRA, A. L. *Comercio electrónico…op., cit.,* p. 22; DE ROSSELLÓ MORENO, R. *El comercio electrónico…*op., cit., pp. 28 y ss; MADRID PARRADA, A*. "*Seguridad en el…"*op., cit.,* p. 170; ROBLES POMPA, J. (dir.). *Práctica y…op., cit*., pp. 241 y ss*;* ALONSO CONDE, A. B*. Comercio electrónico…op., cit.*, pp. 33-34; JULIA BARCELÓ, R. *Comercio electrónico...op., cit.,* pp. 230 y ss; según expresa el Juzgado de Primera Instancia núm. 2, de Castellón, en su sentencia de 25 de junio de 2008, que «en el sistema de criptografía asimétrica cada usuario cuenta con dos claves, una de las cuales es pública, porque se distribuye libremente a través de la red para que todo aquel que tenga interés en mantener una comunicación con su titular pueda conocerla. Pero, además, hay una clave privada, únicamente conocida por su titular, que se corresponde con la pública. La combinación sucesiva de ambas claves de la manera que se describe a continuación permite imputar la autoría de los mensajes a quien dice ser su emisor, y ofrece otro tipo de ventajas como el mantenimiento de la confidencialidad de sus contenidos: 1º) Autentificación, integridad y no rechazo en origen; No rechazo en destino y, 3º) Confidencialidad», (*AC*/2008/1621); MARTÍNEZ LÓPEZ, L.; MATA MATA, Fco; y RODRÍGUEZ DOMÍNGUEZ, R. Mª. "Sistemas de pago…"*op., cit*., p. 68.

[233] RICO CARILLO, M*. Comercio electrónico…op., cit.,* p. 193*;* FERNÁNDEZ GÓMEZ, E. *Comercio...op., cit.,* p. 116; RAMIÓ AGUIRRE, Jorge. La seguridad informática...*op., cit.*, pp. 155-156; ALONSO UREBA, A; y ALCOVER GARAU, G. "La firma electrónica", en MATEU DE

conocida por cualquier usuario a través de di rectorios públicos de fácil acceso[234] y se emplea para descifrar mensajes y para verificar firmas digitales.

La figura 3 muestra el procedimiento sobre la utilización del par de claves (privada y pública) en el que el emisor cifra el mensaje con su clave privada y, una vez cifrado (ininteligible) lo envía al receptor. Éste, al recibir el mensaje, la descifra utilizando la clave pública del emisor. Si el mensaje descifrado es legible e inteligible significa necesariamente que ese mensaje ha sido cifrado con la clave privada del emisor (es decir, que proviene del emisor) y que no ha sufrido ninguna alteración durante la transmisión del emisor hacia el receptor porque si hubiera sido alterado por un tercero, el mensaje descifrado por el receptor con la clave pública del emisor no sería legible ni inteligible. Por último, el emisor no podrá negar haber cifrado el mensaje[235].

Figura: 3. Sistema asimetrico



Fuente: Elaborado por el propio autor

ROS, R. y J. M. CENDOYA MÉNENDEZ DE VIGO (coords). *Derecho de internet…op.cit.* p.182.

[234] MARTÍNEZ NADAL A.: *Comercio electrónico…op., cit.*, p. 42; RUIZ-GALLARDÓN, M.: "Fe pública y contratación telemática…"*op., cit.,* p.105; FONT, A. Seguridad…*op., cit*., p. 55; siguiendo el criterio de éste autor, quien afirma que "la clave pública puede ser transmitida sin encriptar a través de network inseguros, por no ser secreta"; DE QUINTO ZUMARAGA, Fco. *La firma electrónica...op., cit.,* p.102; RICO CARILLO, M*. Comercio electrónico…op., cit.,* p.193*;* ZAGANI, R. *Firma digitale…op., cit.,* p. 44.

[235] GUIJARRO COLOMA, Luis. Fundamentos técnicos...op., cit., p. 238; MARIÑO LOPEZ, A. *Responsabilidad civil*…op., cit., 149 p; HERNANDEZ LAVADO, L. "Contratación…"*op., cit.,* p.153; LLANEZA GONZALÉZ, P. *Internet y...op., cit*., p. 306.

Es difícil conseguir la confidencialidad, de hecho, la firma electrónica no la garantiza como tal. Sin embargo es posible lograr la autenticación, la integridad (certeza de que el mensaje no ha sido alterado) y el no rechazo en origen (imposibilidad de que el emisor niegue que el mensaje recibido por el receptor haya sido cifrado por el emisor con la clave privada de éste)[236].

En este punto la criptografía asimétrica juega un papel fundamental en las transacciones electrónicas. Es decir, el sistema asimétrico se ha convertido en uno de los mecanismos de mayor fiabilidad para garantizar en las transacciones electrónicas la autoría del mensaje, o sea, quien lo envía y la integridad del mismo[237].

Por último y a modo de conclusión se ha de resaltar que la implantación de los sistemas criptográficos en las operaciones de pago efectuadas mediante el uso del número de la tarjeta de crédito o débito en el comercio electrónico a través de Internet desempeña funciones primordiales en lo relacionado con la seguridad de dichas operaciones[238].

Reiterando lo dicho con anterioridad en uno de los párrafos de este capítulo, la finalidad que persigue la criptografía es garantizar el secreto en la comunicación entre las partes intervinientes en una transacción on line y asegurar que la información que se envía es auténtica en un doble sentido: el remitente es realmente quien dice ser y el contenido del mensaje enviado, habitualmente denominado criptograma no ha sido modificado en su tránsito.

---

[236] Vid. MARTÍNEZ NADAL A.: *"Aproximación…op., cit.,* pp. 1-2.

[237] MARIÑO LÓPEZ, A. *R responsabilidad civil*…op., cit., p. 410.

[238] Según sostiene la Profesora RICO CARRILLO, en uno de sus obras, que "en los pagos realizados a través de Internet, la criptografía es una herramienta ideal que proporciona seguridad a la operación, ya que permite ocultar la información que viaja a través de la Red, en estos casos es necesario proteger tanto la información del titular como la información asociada al instrumento de pago", RICO CARRILLO, M. «La protección de los consumidores en las transacciones electrónicas de pago», en *Primera Revista Multimedia Científica de Estudios Telemáticos en Venezuela* vol. 6, núm. 3, 2007 [En Línea] Disponible en Internet: http://www.publicaciones.urbe.edu/index.php/telematique/article/view/835/2043(última consulta 4 de julio de 2012).

2.4. La firma digital y la función hash

Siguiendo la doctrina[239] y la legislación diremos que la firma digital es una aplicación basada en la criptografía de clave pública, especialmente en el ámbito de la contratación electrónica, en la que se proporciona autenticidad, integridad y no rechazo de la información transmitida y de la identidad del transmitente en intercambios económicos en los que las partes no se conocen previamente. La firma digital se crea por medio de clave privada[240] y la clave pública se utiliza para la verificación de la misma[241].

El funcionamiento de la firma digital es básicamente el comentado en el epígrafe anterior, en que el emisor de un mensaje lo cifra digitalmente utilizando su propia clave privada y el receptor sólo puede descifrar el mensaje utilizando la clave pública del primero. De este modo, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la clave privada del emisor.

El procedimiento de la firma digital es el cifrado de un mensaje en claro utilizando un algoritmo de clave pública y haciendo uso de la clave privada.

---

[239] Véanse, DE MIGUEL ASENSIO, P. A.: *Derecho Privado...op., cit.,* p.132; ALCOVER GARAU, G. "Concepto de firma electrónica, firma electrónica y firma digital", en PERALES SANZ, J.L.: *La seguridad jurídica...op., cit.,* p.33; MORENO NAVARRETE, M A.: *Contratos…, op., cit.,* p.105; MARTÍNEZ NADAL A.: *Comercio electrónico…*op., cit., pp. 44-45; ARISTOTELES MAGÁN PERALES, José Mª. "La nueva administración pública electrónica, las relaciones electrónicas entre la administración y el ciudadano. Especial referencia a la firma electrónica", en PUNZÓN MORALEDA, Jesús (coord.). *Administraciones públicas y nuevas tecnologías.* Valladolid: Editorial Lex Nova, S.A., 2005, p. 96; RAMOS SUAREZ, Fernando*. La firma digital: aspectos técnicos y legales* [En línea] Disponible en Internet: http://www.marketingycomercio.com/numero14/00abr_firmadigital.htm(última consulta el 20 de enero de 2012); vid., BIDGODI, H. *Electronic…, op., cit., p.* 206.

[240] Véanse el art. 2.4 de la Directiva 1999/93/CE, en la que se definen los "datos de creación de firma: los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica", en Directiva. 1999/93/CE del Parlamento Europeo y del consejo, de 13 de diciembre de 1999, por lo que se establece un marco comunitario para la firma electrónica, publicado en el *DO* nº L 013 de 19 de enero de 2000, pp.12-20.

[241] Vid. art. 2.7, reseña que los datos de verificación de firma son:" códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica", en Directiva 1999/93/ CE…*op., cit.,* pp.12-20; MARIÑO LÓPEZ, A. *Responsabilidad civil…op., cit.,* p.147*;* MADRID PARRA, A. "Seguridad en…"*op., cit*., p.131.

Sin embargo, uno de los inconvenientes que presentan los algoritmos de clave pública o asimétrica consiste en la pérdida de velocidad, lo que los hacen más lentos que los algoritmos simétricos[242] porque crecen con el tamaño del mensaje a cifrar y tienen un coste muy elevado[243]. Por ello, la firma digital de un documento se realiza de forma distinta[244].

De hecho, es necesario aclarar que la firma digital de un documento no se realiza mediante el cifrado del mismo usando la clave privada del emisor, sino mediante el cifrado del resumen del texto generado a través de un algoritmo de resumen de texto[245]. Es decir, la firma digital hace uso de la "función hash" que no es más que una función matemática que se aplica sobre un conjunto de datos o documentos de cualquier tamaño y, como resultado, se obtiene otro de tamaño reducido[246], en ocasiones denominado "resumen o digest" de

[242] RICO CARILLO, M*. Comercio electrónico…op., cit*., p.203*;* FERNÁNDEZ GÓMEZ, E. *Comercio...op., cit.,* p.116*.*

[243] LLANEZA GONZALÉZ, P. *Internet...op., cit.,* p. 306.

[244] GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit*., p. 240.

[245] Vid. ALONSO UREBA, A; y ALCOVER GARAU, G. "La firma electrónica, en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital.* Prólogo de Ana Birulés I Bertrán Elcano (Navarra): Aranzadi, 2000. pp.182 y ss; BARRAL VIÑALS, I. *La seguridad en*…op., cit., p. 86.

[246] Siguiendo el criterio sostenido por el profesor ILLESCAS ORTIZ, quien señala en uno de sus obras, que la función *hash* «comprime o reúne firma electrónica y mensaje de datos en un resultado (MD) electrónico repetible tantas veces cuantas se use los mismos ingredientes, hace imposible el conocimiento de mensaje de dato (MD) que lo integra y no puede ser nunca objeto de confusión con otro mensaje de dato (MD)», en ILLESCAS ORTIZ, R. *Derecho de la…op., cit.*, p. 93, nota 69; FERNÁNDEZ GÓMEZ, E. *Comercio...op., cit.,* p. 116; DE QUINTO ZUMARAGA, Fco. *La firma electrónica...op., cit.,* 105 p; la *Recomendación de la Unión Internacional de Telecomunicaciones, UIT-T.X.810(1995 S),* define el «hash o la huella dactilar como la característica de un ítem de datos, por ejemplo un valor de comprobación criptográfico o el resultado de la ejecución de una función de cálculo unidireccional sobre los datos, que suficientemente peculiar del ítem de los datos y que no es factible, mediante cálculo, hallar otro ítem de datos que posea las mismas características; asimismo define la *función unidireccional* como aquella función (matemática) cuyo cálculo es fácil, pero que, cuando se conocen un resultado, no es factible, mediante cálculo, hallar cualquiera de los valor que pueden haber sido suministrado para obtenerlo», citado por MARTÍNEZ NADAL A.: *Comercio electrónico…*op., cit., p. 48, nota 30; y LLANEZA GONZALÉZ, P.: *Internet…op., cit*., p. 306, nota 307; RICO CARILLO, M*. Comercio electrónico…op., cit.,* p. 203*;* ALCOVER GARAU, G. «Concepto de firma electrónica, firma electrónica y firma digital», en PERALES SANZ, J.L. *La seguridad jurídica* en las transacciones electrónicas. Seminario organizado por el Consejo General del Notariado en la UIMP. Madrid: Civitas, 2002, p. 33; FORCADA MIRANDA, Francisco Javier. "El registro de

los datos originales, de longitud fija (entre 128 ó 160 bits) e independiente de la longitud original. Como hemos adelantado con anterioridad, lo que se cifra es el resumen con la clave privada del ente emisor que sólo puede ser verificada con la clave pública.

Además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes que produzca la misma secuencia hash[247]. Cualquier alteración o modificación en el contenido del mensaje por mínima que sea supondría un cambio en el hash o "resumen", es decir, en la firma que se obtendría al aplicar de nuevo el algoritmo, reflejando que el mensaje ya no es el mismo[248]. Los algoritmos hash más utilizados son el MD5 de RSA ó SHA-1.

Cabe destacar que la "función hash" tiene como finalidad simplificar la firma digital del mensaje cuando éste es muy largo. Es decir, con la función hash el mensaje no se encripta sino que su finalidad es comprimir los textos para que el receptor pueda comprobar la integridad del mismo con mayor rapidez. Al aplicar la firma digital se encripta sólo la función hash y no todo el documento, lo que permite que a la hora de descifrar el mensaje el proceso dure menos tiempo.

---

propiedad y las nuevas tecnologías. La publicidad formal. Acceso al proceso y efectos jurídicos", en ALMENAR BELENGUER, Manuel; CARBONELL LLORENS, Cristina. *Jurisdicción y registro de la propiedad y mercantil: nuevas áreas de interés común*. Madrid: Consejo General de Poder Judicial, 2004, p.108; BARRIUSO R, C.: *Contratación....op., cit*., p. 405; JULIA BARCELÓ, R. *Comercio electrónico...op., cit.,* 233 p; LOMASCOLO SZITTYAY, R.: *Aspectos técnicos de...op., cit.,* p. 69, vid. AZOFRA VEGAS, Fernando. «La contratación electrónica bancaria», en *RDBB*, núm. 68, octubre-diciembre 1997, pp. 111 y ss.

[247] Como señala la doctrina, el hash es irrepetibles al igual que la huella digital de las personas, que lo hace único en el mundo. Así pues, cada documento se le asigna un hash. [En línea] disponible en Internet: http://ciberhabitat.gob.mx/comercio/firma/index.html (última consulta el 2 de febrero de 2012); vid. BARRIUSO RUIZ, C.: *Contratación....op., cit*., p.405.

[248] MARTÍNEZ NADAL A.: *Comercio electrónico…*op., cit. pp. 47- 48; ARISTOTELES MAGÁN, J. Mª. "La nueva administración*…op., cit.,* pp. 96 y ss.

2.4.1. Generación y verificación de la firma digital

En el procedimiento de utilización de la firma digital concurren dos procesos sucesivos que consisten en: A) Generación de la firma del mensaje por el emisor del mismo; y B) Verificación de la firma digital por el receptor del mensaje.

A. Generación de firma digital

El proceso de generación de la firma digital se representa en la Figura 4. Se inicia con la obtención de un mensaje en claro escrito por el emisor en el que éste aplica a ese mensaje una función hash o resumen, mediante la cual obtiene un resumen del mensaje. Al finalizar esa aplicación, el emisor cifra digitalmente ese mensaje comprimido utilizando su clave privada, es decir, lo firma[249].

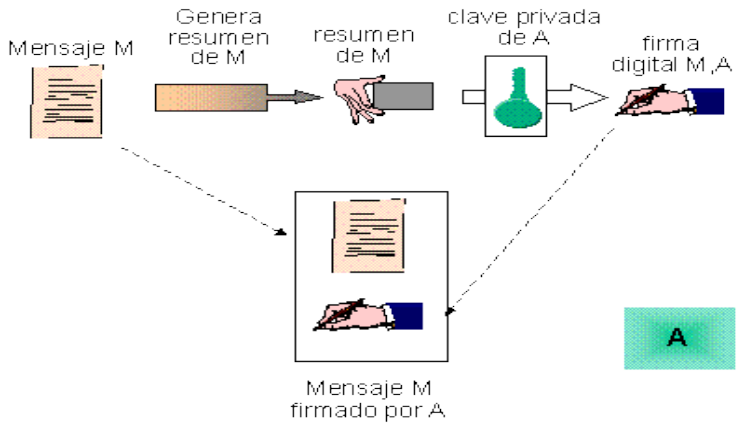
A continuación, el emisor envía el mensaje firmado (comprimido) junto con el mensaje en claro al receptor quien deberá proceder a la verificación de la firma. Este último recibe el mensaje con los siguientes elementos:

a) El mensaje inicial (mensaje en claro)

b) La firma del mensaje, que a su vez se compone de dos elementos: el hash o "mensaje-resumen" cifrado y la clave privada del emisor.

[249] Véanse COUTO CALVIÑO, R. *Servicios de certificación de…op., cit.,* pp.34 y ss; ARISTOTELES MAGÁN, J. Mª. "La nueva administración*…"op., cit.,* p. 97; MARTÍNEZ NADAL A.: *Comercio electrónico…op., cit*., p.47.

Obsérvese la Figura 4, sobre generación de la firma digital.



Fuente: Enrique Vásquez Callao, y Julia Berrocal Colmenarejo

B. Verificación de la firma digital

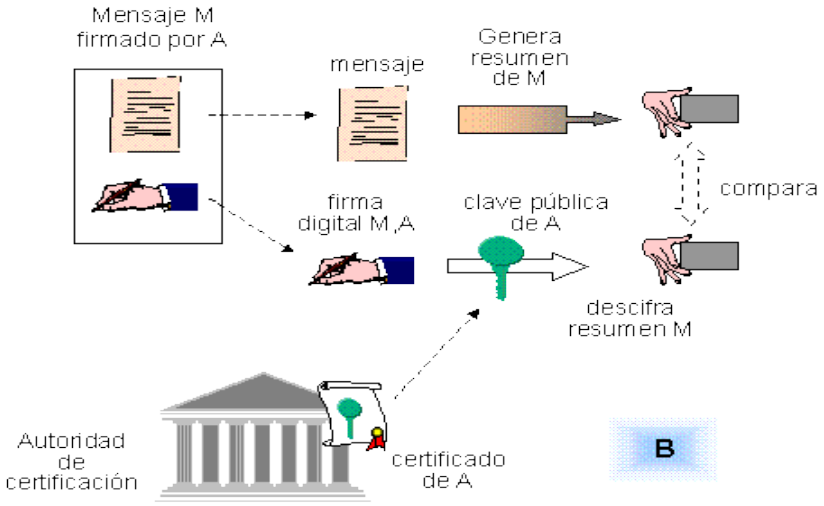
Una vez estudiado cómo se firma digitalmente un documento o mensaje electrónico se plantea una interrogante. ¿Cómo se puede verificar dicha firma digital? Existen diversas opciones para la verificación de la misma, sin embargo, hay que tener en cuenta que para que el receptor del mensaje electrónico proceda a la verificación de la firma digital, una vez que reciba el mensaje, es necesario que posea la clave pública del emisor; teniéndola puede iniciar la verificación de la firma digital de la siguiente manera:

El primer paso para la verificación de la firma digital se refleja en la Figura 5 que consiste en que el destinatario o receptor aplica la clave pública del emisor para descifrar el hash firmado con la clave privada del mismo y así obtiene el resumen[250]. En el siguiente paso, el receptor aplicará al mensaje, que aparece en claro o no cifrado, la misma función hash que utilizó el emisor con anterioridad obteniendo igualmente un mensaje-resumen. Si el mensaje ha sido cifrado para garantizar la confidencialidad del mismo, previamente el receptor deberá descifrarlo utilizando para ello su propia clave privada.

[250] MARTÍNEZ NADAL A.: *Comercio electrónico…*op., cit., 48 p; LLANEZA GONZALÉZ, P.: *Internet...op., cit.,* p. 306.

De este modo, el receptor compara el hash recibido y descifrado y el hash obtenido por él mismo. Si ambos coinciden totalmente significa que el mensaje no ha sufrido modificación durante su transmisión[251], es decir, es íntegro o auténtico. El hash descifrado por el receptor con la clave pública del emisor ha sido necesariamente cifrado con la clave privada del emisor y, por tanto, proviene del emisor.

Fig. 5. Verificación de la firma digital



Fuente: Enrique Vásquez Callao, y Julia Berrocal Colmenarejo

Por el contrario, si ambos hash o " mensajes-resumen" no coinciden quiere decir que el mensaje ha sido alterado por un tercero durante el proceso de transmisión[252] y si el mensaje-resumen descifrado por el receptor es ininteligible quiere decir que no ha s ido cifrado con la clave privada del emisor. Por lo que el mensaje no es auténtico o n o ha sido firmado por el emisor sino por un tercero ajeno al proceso.

[251] Vid. MARTÍNEZ NADAL A.: *Comercio electrónico…*op., cit., pp. 48-49; VASQUEZ CALLAO, E.; BERROCAL COLMENAREJO, J. *Comercio electrónico...op., cit.,* p. 20; FERNÁNDEZ GÓMEZ, E. *Comercio...op., cit.,* p.116; DE QUINTO ZUMARAGA, Fco. *La firma electrónica...op., cit.,* p.105; COUTO CALVIÑO, R. *Servicios de certificación de…op., cit.,* p.35*;* ARISTOTELES MAGÁN, J. Mª. "La nueva administración*…op., cit.,* p.97*;* BARRIUSO RUIZ, C.: *Contratación....op., cit*., p. 405.

[252] LLANEZA GONZALÉZ, P.: *Internet...op., cit.,* p. 306.

Debemos destacar que para que funcione correctamente el sistema es necesario que el mismo garantice la autenticación de las partes (que éstas son quienes dicen ser). Si dicho requisito no llega a cumplirse estaríamos ante la imposibilidad de poder acreditar la identificación del ente emisor del mensaje[253]. Para evitar este tipo de situación es imprescindible la existencia de una tercera parte de confianza (prestador de servicios de certificación) que certifique e identifique que un sujeto es el verdadero titular de la clave pública y registre a ese sujeto como el titular de la clave mencionada[254]. Sobre esta cuestión desarrollaremos un apartado más adelante.

Como hemos señalado a lo largo de este epígrafe, el sistema de la firma digital se utiliza como mecanismo de seguridad en las comunicaciones electrónicas, especialmente a través de Internet, para garantizar la autenticación, integridad y el no repudio de origen de los documentos electrónicos. Además, se basa en la utilización de diversas aplicaciones telemáticas tales como el acceso seguro a servidores web, el pago mediante tarjeta de crédito o débito en Internet con protocolo SSL, SET y 3D secure, entre otras[255].

A continuación examinaremos las distintas clases de protocolos que garantizan la seguridad en las operaciones de pago mediante el uso del número de la tarjeta en Internet: cómo funcionan, sus ventajas e inconvenientes así como las posibles diferencias existentes entre ellos. Estos

[253] MARIÑO LOPEZ, A. *Responsabilidad civil*…op., cit., p. 150.

[254] MARIÑO LOPEZ, A. *Responsabilidad civil…op., cit*., p.151; ARISTOTELES MAGÁN, J. Mª.: "La nueva administración*…op., cit.,* p. 98; compartiéndonos el criterio de MANUEL VIILLAR, en la que este señala que "la firma digital no identifica por sí sola el autor de un mensaje ya que sólo confirma que el clave privada utilizada para firmar el mensaje corresponde la clave pública que permite descifrarlo, sino solo por medio de un complemento de certificado electrónico, que consta que la clave pública pertenece a quien dice haberlo hecho", MANUEL VIILLAR, José. "Una aproximación a la firma electrónica", en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet Contratación electrónica y firma digital.* Prólogo de Ana Birulés I Bertrán Elcano (Navarra): Aranzadi, 2000, p. 170; BRIZ, J.; y LASO, I. *Internet y comercio...op., cit.,* p. 397.

[255] Vid. GUIJARRO COLOMA, L. "Fundamentos técnicos..."*op., cit*., p. 244.

protocolos ofrecen seguridad y proporcionan la confianza que consumidores y usuarios demandan en sus transacciones en Internet.

Se ha de hacer hincapié, que no siempre se usa firma electrónica en la contratación, pero sí los protocolos de seguridad en el pago.

2.5. Protocolos de seguridad para la realización de pago mediante el uso del número de las tarjetas a través de Internet

2.5.1. Aspecto general

El uso de la tarjeta como medio de pago en un establecimiento comercial donde se presenta físicamente puede representar un riesgo aunque de otro tipo, por eso se ha extendido la práctica de solicitar el DNI o el NIE[256]. Con respecto, ciertamente a la transmisión de los datos, el Banco con la entrega de TPV asegura niveles de seguridad.

Igualmente, el uso de la misma en el comercio electrónico (en una tienda virtual) donde se encuentran ausente las partes intervinientes conlleva un riesgo, por lo que es necesario un mecanismo tecnológico que garantice que se da la correcta manipulación y transmisión de los datos relativos a la tarjeta de pago con la finalidad de evitar el uso fraudulento[257].

Por tal razón, se han creado diversos «mecanismos» o « protocolos», útiles para garantizar la seguridad en las transacciones realizadas a través de redes abiertas como Internet, donde se hace uso de diferentes procedimientos para pagar con tarjeta de forma segura[258]. Por ello, estos protocolos SSL (Secure Socket Layer), SET (Secure Electronic Transaction) y

[256] NIE (significa número de identidad del extranjero). Es la documentación que el Gobierno español otorgan a los extranjeros residentes en España.
[257] VICENTE BLANCO, D.J. "Medios de pago..."*op., cit*., p.278.
[258] Ibídem,

3D Secure establecen mecanismos de seguridad que sirven para la comunicación de interlocutores en el pago con tarjetas.

Antes de analizar los referidos protocolos de seguridad o criptográficos que se usan en el comercio electrónico, nos gustaría preguntarnos ¿qué es lo que entendemos por protocolo de seguridad? Como señala la doctrina, el protocolo de seguridad es un conjunto de mensajes intercambiados entre dos o más partes intervinientes en una transacción[259]. Estos protocolos regulan el intercambio de información entre el comprador, el vendedor y las entidades financieras (bancos o intermediarios) con el fin de establecer una comunicación inteligente para ambos servidores[260].

Por otra parte, se puede definir el protocolo como un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (emisor y receptor). Estos protocolos «gobiernan» formatos, modos de acceso, secuencias temporales, etc. O sea, el protocolo es el lenguaje (conjunto de reglas formales) que permite comunicar nodos (computadoras) entre sí. Existen infinidad de protocolos (a nivel de aplicación) en internet u otras redes, por ejemplo: HTTP, FTP, TCP, POP3, SMTP, SSH, IMAP, etc[261].

2.5.2. Protocolo SSL (Secure Sockets Layer)

Es un protocolo de seguridad desarrollado por Netscape Communications Corporation que dispone de un nivel seguro de transporte entre el servicio

[259] DÍAZ, Gabriel; MUR, Francisco. *Seguridad en las comunicaciones y en la información*. Madrid: Universidad Nacional de Educación a Distancia, 2004, p.371; coincidiéndonos con la definición que da GÓMEZ VIEITES, en la que este señala que los protocolos criptográficos "son algoritmos distribuidos que constan de una secuencia de pasos o etapas que tienen que ser realizados por dos o más entidades para alcanzar unos determinados objetivos de seguridad", en GÓMEZ VIEITES, Álvaro. *Enciclopedia de la seguridad informática*. Madrid: RA-MA, 2006, p. 356.

[260] MARTÍNEZ GONZÁLEZ, M. "Mecanismo de seguridad…"*op., cit*., p.52.

[261] LWP Comunidad de Programadores [En línea] disponible en Internet: http://www.lawebdelprogramador.com/diccionario/buscar.php?cadena=protocolo&x=39&y=6 (última consulta, 26 de noviembre de 2012).

clásico de transporte en Internet (TCP/IP) y las aplicaciones que se comunican a través de él. Es el sistema más usado, posee facilidad de uso y requerimientos técnicos al estar instalado en los propios navegadores y no necesita usar un software específico.

El sistema SSL sirve para cifrar la información intercambiada en Internet entre el ordenador del cliente y el propio servidor utilizando conjuntamente cifrados simétricos (DES, RC4, etc.) y asimétricos (RSA, DSS, etc.)[262] con el objetivo de impedir que un tercero no autorizado pueda tener acceso a los datos. Además, este sistema permite la autenticación y privacidad de la información entre extremos en Internet mediante el uso de criptografía. No obstante, sólo garantiza la autenticación del servidor (vendedor)[263] ; es decir, garantiza su identidad mientras que el cliente se mantiene sin autenticar (es opcional)[264], situación que puede traer consigo que una persona ajena que se apodere del número de tarjeta y el NIP pueda realizar transacciones en Internet.

[262] Vid. MADRID PARRA, A. "Seguridad en el…", *op., cit.,* p.170; RICO CARRILLO, M. *Comercio electrónico…op., cit.,* p.216; GÓNZALO ÁLVAREZ, M. "Compras seguras en la red publicado", en *PC Word digital***,** el 1 de octubre de 2004, [En línea] disponible en internet:http://www.idg.es/pcworld/Compras_seguras_en_la_Red/art161637.htm-74(última consulta, el 10 de marzo de 2012); vid. RODRÍGO GONZÁLEZ, Oscar. *Comercio electrónico*. Madrid: Grupo Anaya, S.A., 2008, pp. 180 y ss; BIDGODI, H. *Electronic commer. Principles…, op., cit.,* 208.

[263] El vendedor debe tener un certificado emitido por una Autoridad de Certificación, por ejemplo Verisign, que es la entidad externa del máximo prestigio a nivel mundial en la provisión de Infraestructuras de Clave Pública y en la emisión de Certificados. (http://www.verisign.com); en caso de España la entidad bancaria Banesto presta diversos servicios de certificación dirigidos a incrementar la seguridad y confianza en las relaciones telemáticas; así emite certificados digitales X.509 v.3 de carácter reconocido, que permiten generar firma electrónica avanzada; sobre este aspecto véanse FLORES DOÑA, M.ª De La Sierra, en FERNÁNDEZ RUIZ, José Luis (dir). *Impacto del comercio electrónico en el derecho de la contratación*. Madrid: Editoriales de Derechos Reunidos, S.A., p.166; ESCOBAR ESPINAR, M. *Contratación...op., cit.,* p.169; BRIZ, J.; y LASO, I. *Internet y comercio...op, cit.,* p. 382.

[264] DÍAZ, G.; MUR, Fco.; y SANCRISTÓBAL, E.: *Seguridad en...op., cit.,* p. 379*;* FONT, A. *Seguridad...op., cit*., p. 66; FERNÁNDEZ GÓMEZ, E. *Conocimientos...op., cit.,* p. 221; VILA SOBRINO, José Antonio. "Fundamentos técnicos. Aspectos técnicos para el desarrollo de aplicaciones de comercio electrónico", en GOMÉZ SEGADE, J.A (dir.). *Comercio en Internet*. Madrid: Marcial Pons, 2001, p. 57.

El protocolo SSL permite a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir la falsificación de la identidad del remitente (phishing) y mantener la integridad del mensaje[265]. Tal como habíamos señalado en el párrafo anterior, el sistema SSL autentica los servidores, encripta las comunicaciones y preserva la integridad del mensaje[266]. Pero, sin embargo, no ofrece la garantía de que una de las partes pueda repudiar con posterioridad la operación[267]. Se ha de señalar que con el sistema SSL se crea una conexión segura cliente-servidor a la hora de efectuar transacciones electrónicas[268].

2.5.2.1. *Funcionamiento de SSL*

Las comunicaciones tienen lugar en dos fases. En una primera fase se negocia entre el cliente o navegador (del comprador) y el servidor (del proveedor de bienes o servicios). Una vez que se pactan los parámetros de la comunicación, el servidor se autentica ante el cliente y se acuerda una clave simétrica sólo válida para esa sesión[269]. En una segunda fase se transfieren

[265] BARRIUSO RUIZ, C.: *Contratación....op., cit*., p.616.

[266] MARTÍNEZ NADAL. A. "Medios de pago..."*op., cit.,* p.7. [266] DÍAZ, G; MUR, Fco *Seguridad en...op., cit.,* p. 379*;* FONT, A. *Seguridad...op., cit*., p. 66; FERNÁNDEZ GÓMEZ, E. *Conocimientos...op., cit.,* p. 221; VILA SOBRINO, J A. "Fundamentos técnicos…"op., cit., p. 57.

[266] BARRIUSO RUIZ, C.: *Contratación....*op., cit., p.616.

[267] VELCHES TRASSIERA, Antonio J.: *Aproximación a la sociedad de la información: firma digital, comercio y banca electrónica.* Madrid: Centro de Estudios Registrales, 20002, pp. 82 y ss; BRIZ, J.; y LASO, I. *Internet y comercio...*op., cit., p.382*.*

[268] Vid. BARRIUSO RUIZ, C.: *Contratación*…op., cit., p. 456. Para este autor, "el sistema SSL, cifra los datos que entra y salen del servidor (https) hacia o des de el cliente, la información enviada llegará de manera privada, confidencial e integra al servidor del lado del cliente, se garantiza que el sitio web es auténtico con lo que se evitaría el phishing o la suplantación del web"; GARCÍA, M., *Autenticación y cifrado para un comercio electrónico*. [En Línea] Disponible en Internet: http://www.esegi.es (última consulta 30 mayo de 2011); en este sentido el Profesor MADRID PARRA califica al sistema *SSL*, de "un sistema de encriptación que evita que terceras personas puedan ver o modificar los datos que se transmitan a través de la red (Internet). funciona de forma que el navegador del cliente cifra automáticamente, la información de la orden de pago antes de enviarla al comercio o, en caso que utilice un TPV virtual, a la entidad financiera. Una vez enviada, únicamente el destinatario podrá tener acceso a e sta información, que q uedara protegida", MADRID PARRA, A. "Seguridad en el…"*op., cit.,* p.163.

[269] Vid. MARTÍNEZ GONZÁLEZ, M. "Mecanismo de seguridad…"*op., cit.,* p. 53.

los datos cifrados con dicha clave. Este sistema es transparente para las aplicaciones finales, que simplemente saben que el canal se encarga de proporcionarles confidencialidad entre los extremos.

El sistema se basa en la utilización de un mecanismo de claves públicas. Así, el navegador incluye de ant emano las claves públicas de ciertas Entidades Certificadoras Autorizadas (ECA); de esta forma, se pone en comunicación con un servidor seguro que le envía su clave pública rubricada por la ECA correspondiente. La identificación se completa enviando al servidor un mensaje aleatorio que éste debe firmar, y así el cliente sabe que el proveedor es quien dice ser.

Verificada la identidad del servidor, el cliente genera una clave de sesión y la envía cifrada con la clave pública del servidor. Conociendo ambos la clave de sesión, se intercambian los datos cifrados por el algoritmo de clave secreta.

Existen varias alternativas al SSL pero se puede considerar que este protocolo es el auténtico estándar para conexiones seguras, aunque con ciertas limitaciones en el caso de utilizar tarjetas de crédito ya que lo único que hace es impedir que la información compartida por el navegador y el servidor pueda ser observada por un tercero, pues no está diseñado para interacciones entre múltiples partes.

2.5.2.2. *Sujetos intervinientes en la transacción por medio de SSL*

Generalmente son dos entes los que intervienen: el titular de la tarjeta (Cardholder) y el proveedor de servicios, bienes o establecimiento (Merchant), quien acepta la tarjeta como medio de pago electrónico.

2.5.2.3. *Ventajas e Inconvenientes del sistema SSL*

Una de las ventajas del protocolo SSL es que en cada sesión se negocia una clave de sesión diferente, lo cual aumenta la seguridad; otra ventaja es que no requiere de la instalación de un software ya que la mayoría de los servidores lo poseen, por ejemplo Explorer y Netscape. Además, el SSL es el sistema de protocolo con más uso para pagos electrónicos.

Sin embargo, sus inconvenientes o limitaciones derivan precisamente de que no es un protocolo diseñado específicamente para el comercio electrónico, sino para proporcionar seguridad en la comunicación entre servidores web y navegadores web o browser[270].

Como señalan algunos autores[271], este tipo de protocolo no permite ir más allá de la autenticación y seguridad de la comunicación ya que no comprueba si el cliente está autorizado a pagar con tarjeta o no, ni el tipo de pago que tanto cliente como comerciante pueden realizar, ni otras informaciones similares. Esto deja abierto el camino para posibles fraudes como la compra con tarjetas robadas o el repudio; tampoco protege las transacciones donde interviene el emisor de tarjetas, lo único que hace es asegurar la interacción entre comprador y vendedor cuando los datos viajan desde el navegador hasta el servidor.

Además, los comerciantes o proveedores de bienes o servicios corren el riesgo de que el número de tarjeta que les proporcione el cliente sea fraudulento. De ser así, asumirían los gastos de las transacciones fraudulentas[272]. Situación que anima a las entidades de crédito a añadir una comisión en las compras bastante elevada (un 5% aproximadamente) para

[270] FONT, A. *Seguridad...op., cit*., p.65.
[271] MARTÍNEZ GONZÁLEZ, M. "Mecanismo de seguridad…" *op., cit*., pp.55 y ss;
[272] RICO CARRILLO, M. *Comercio electrónico...*op., cit., p. 216; VELCHES TRASSIERA, A. J.: *Aproximación a la...op., cit*., p.30; BRIZ, J.; y LASO, I. *Internet y comercio...op., cit.,* p.384.

compensar este tipo de fraude. Esto hace que el precio de la compra se incremente considerablemente, lo que anula el atractivo inicial de comprar por Internet: los precios bajos.

Tampoco protege al comprador del riesgo de que el proveedor de bienes o servicios pueda realizar cualquier tipo de fraude con la finalidad de conocer su número de tarjeta ya que no queda garantizada la integridad del documento de pago[273].

2.5.2.4. *Servidores seguros*

¿Cómo podemos asegurarnos que el sitio web en el que pretendemos hacer la compra es seguro o utiliza cifrado? Para que el cliente esté seguro de que un servidor en el que navegamos usa el sistema de seguridad SSL se deben tener en cuenta los requisitos a continuación enumerados[274].

Primero, recibiremos un mensaje donde nos advierten que estamos a punto de ver las páginas bajo una conexión segura y que todas las informaciones que intercambiamos con ese sitio no podrán ser vistas por nadie más en la web; también aparecerá la figura de un candado cerrado o llave en la parte inferior izquierda[275].

En segundo lugar, para identificar el SSL debemos observar la barra de direcciones antes de introducir nuestros datos. Se cambia de un http:// a un https:// (Hipertext Transpot Protocol Secure) donde la "s" significa que el sitio es seguro. Por ejemplo:

https://www.citapreviadni.es; https://www.aranzadi.es.

[273] ALVAREZ MARAÑO, G. *Seguridad en el comercio electrónico: ¿SSL O SET?* [En línea] disponible en Internet: http://www.iec.csic.es/CRIPTONOMICON/susurros/susurros08.html-(última consulta 2 de mayo de 2012); BRIZ, J.; y LASO, I. *Internet y comercio...op., cit.,* p.384.

[274] DÍAZ, Gabriel; MUR, Fco. *Seguridad en...op., cit.,* p.375.

[275] ESCOBAR ESPINAR, M. *El comercio…op., cit*., p.178.

Una vez cumplidos estos requisitos, podemos confiar en que estamos conectando con un servidor web que hace uso del protocolo SSL[276]. En el caso de que no se den estos requisitos, no sería aconsejable comprar con tarjeta de crédito o débito, ya que la tienda virtual o servidor en la que pretendemos hacer la compra no son seguros, por lo que los datos de la tarjeta viajan sin encriptar por la red. Así pues, estamos corriendo el riesgo de que estos datos pueden ser interceptados por un tercero no autorizado con la finalidad de hacer un uso ilegitimo de ellos.

La seguridad en el sistema SSL depende de la confianza que el cliente tenga en el proveedor de bienes o servicios (vendedor), ya que, como hemos señalado en uno de los epígrafes anteriores, el vendedor puede realizar cualquier tipo de fraude. Sólo las empresas con muy buena reputación podrían, a priori, contar con esta confianza del consumidor.

El sistema SSL utiliza certificados digitales siguiendo el estándar X.509, es decir, certificados de propósito general. Sería más interesante que existieran autoridades certificadoras creadas especialmente para emitir certificados de este tipo y que dichas autoridades estuvieran avaladas por la banca, de tal modo que los certificados digitales expedidos tuvieran conexión con cuentas bancarias concretas.

2.5.3. Protocolo SET (Secure Electronic Transaction)

El protocolo SET[277] fue creado en 1995 por las grandes empresas propietarias de marcas de tarjetas (Visa Internacional y MasterCard Internacional) con la colaboración de otras compañías líderes en el mercado

[276] LAFUENTE SÁNCHEZ, R. *Los servicios*… op., cit., p. 37; teniendo en cuenta dichas condiciones se pueden facilitar los datos de la tarjeta de crédito sin peligro, éstos viajarán de forma cifrada al comercio, garantizando la privacidad y confidencialidad del proceso; MARTÍNEZ GÓNZALEZ, M.: "Mecanismo de seguridad*…"op., cit.,* p.53.

[277] Véase al respeto: http://www.secto.org (última consulta, 27 de no viembre de 2012); VILA SOBRINO, J. A. "Fundamentos…", *op., cit.,* p. 58; BRIZ, J.; y LASO, I. *Internet y comercio...op., cit.,* p.382; VILLAR VARELA, Ana Mª. *Comercio electrónico. Conceptos, recursos y estrategias*. Vigo: Ideaspropias, 2005, p.108.

de las tecnologías de la información, como Microsoft[278], IBM[279], GTE, Netscape Comunication Corp.[280], SAIC, y Sistema VeriSign[281], entre otras[282], con el objetivo de garantizar un uso seguro de pagos con las tarjetas, ya sean de crédito o débito, a través de medios de comunicación inseguros como es el caso de Internet[283], eliminando así los inconvenientes que presenta el sistema SSL.

Como indica la doctrina, el protocolo SET[284] tiene como objetivo garantizar la autenticación de todas las partes que intervienen en la transacción cuando se utilizan las tarjetas de crédito y de débito como medios de pago en Internet; también garantiza la integridad[285] de la información intercambiada que, como el número de tarjeta, no podrá ser alterada de manera accidental o maliciosa durante su transporte a través de r edes telemáticas. Para lograrlo, el mensaje se cifra y se firma sin que la otra parte tenga acceso a los datos y a la confidencialidad de la información; es decir, permite garantizar la seguridad del pago en Internet utilizando el sistema asimétrico o de clave pública, firma digital y certificado electrónico[286].

[278] http://www.microsoft.com (última consulta 27 de noviembre de 2012).
[279] http://www.ibm.com (última consulta 27 de noviembre de 2012).
[280] http://www.netscape.com (última consulta 27 de noviembre de 2012).
[281] http://www.verisign.com (última consulta 27 de noviembre de 2012).
[282] Vid. BARRIUSO RUIZ, C. *Contratación…*op., cit., pp. 455 y ss.
[283] INZA, Julián. "Banca electrónica. Sistema de pagos avanzados", en ILLESCAS ORTÍZ, R (dir.). *Derecho del comercio electrónico.* Madrid: La ley, 2001, pp. 260-267; DE ROSSELLÓ MORENO, Rocío. *El comercio…*op., cit., pp.33-34; RICO CARRILLO, M. *Comercio electrónico…op., cit.*, p. 213; ESCOBAR ESPINAR, M. *El comercio comercio…op., cit.,* p.170.
[284] Vid. FRAMIÑAN SANTAS, J. "Pagos en la red…"*op., cit.,* pp. 378 y ss; RICO CARRILLO, M. *Comercio electrónico…op., cit.*, p. 213; RICO CARRILLO, M. *Comercio electrónico…op., cit.*, p. 213; FERNÁNDEZ GÓMEZ, E. *Conocimientos...op., cit.,* p. 220; BIDGODI, H. *Electronic commer. Principles…op., cit., pp.* 210 y ss.
[285] ÁLVAREZ MARAÑON, Gonzalo. SET a fondo Secure Electronic Transaction, *La Revista de Tecnología y Estrategia de Negocio en Internet (RTENI*), múm.22, 12 de enero de 1999 [En Línea] Disponible en Internet: http://www.idg.es/iworld/articulo.asp?id=103068&sec=iworld-92k (última consulta el 2 de mayo de 2012); VILLAR VARELA, A. *Comercio electrónico…op., cit.,* pp. 108 y ss.
[286] VASQUEZ CALLAO, E. y BERROCAL COLMENAREJO, J. *Comercio electrónico...*op., cit*.,* p. 23; FERNÁNDEZ GÓMEZ, E. *Conocimientos y aplicaciones...*op., cit., p. 220.

2.5.3.1. *Servidores seguros*

¿Cómo podemos asegurarnos que estamos ante un servidor o TPV Virtual seguro? Independientemente del sistema de seguridad implementado, un usuario tendrá la certeza de que el sitio web de la tienda en la que navega es seguro cuando se den las siguientes condiciones:

- ✓ Cuando se añade una "s" de seguro a la dirección del sitio web, por ejemplo: https://

- ✓ Cuando exista un candado amarrillo cerrado o una llave en la parte derecha de la barra del navegador. Si utilizamos Netscape Navigator, aparecerá una llave "entera" en la parte inferior izquierda de la barra de navegación.

Cuando se den estos requisitos, se pueden facilitar los datos de la tarjeta de crédito sin temor a que el mensaje puede ser interceptado ya que viajarán de forma cifrada al comercio, garantizando la privacidad y confidencialidad del proceso[287].

2.5.3.2. *Entes intervinientes en una operativa de pago con tarjeta de crédito en la que se hace uso del SET*

A diferencia del protocolo SSL en el que intervienen dos entes, el cliente (*Cardholder*) y el proveedor de bienes o servicios *(Merchand),* en el protocolo SET intervienen otros sujetos que son necesarios para la transacción electrónica mediante la tarjeta de crédito o débito:

1. *El cliente (Cardholder)*: titular de la tarjeta de crédito o débito.

[287] Sobre este punto véanse a LAFUENTE SÁNCHEZ, R. *Los servicios*… op., cit., p. 244; ESCOBAR ESPINAR, M. *El comercio…op., cit.*, p. 178.

2. *El proveedor de bienes o servicios (Merchant):* comercio o establecimiento que ofrece el producto en su tienda virtual (web).

3. *La entidad emisora de la tarjeta (Issuer):* emite la tarjeta del cliente, extiende su crédito y es responsable de la facturación, recolección y servicio al consumidor.

4. *El Banco adquiriente (Adquirer*): banco con el que el proveedor de bienes o servicios establece una cuenta bancaria y procesa las autorizaciones de pago por tarjeta de crédito[288].

5. *Autoridad de certificación:* aquella que emite los certificados digitales usados como medio de autenticación de las entidades que intervienen directamente en la operación. Pueden ser entidades independientes autorizadas, bancos o los mismos propietarios de la marca de la tarjeta.

6. *El procesador (redes de medios de pago*): proporciona servicios adicionales operando la infraestructura de telecomunicaciones sobre las que se realizan las transacciones.

7. *La pasarela de pagos (Gateway o Terminal de Punto de Venta Virtual)*[289]*:* mecanismo que procesa y autoriza las transacciones del proveedor de bienes o servicios en Internet[290], permite el cobro de las

[288] ESCOBAR ESPINAR, M. *El comercio…op., cit*., p.171; VILA SOBRINO, J. A. «Fundamentos... »*op., cit*., p.57.

[289] MADRID PARRA, A. "Seguridad en el...", *op., cit.,* p.164; PLAZA PENADÉS, J. "Contratación*…", op., cit*., p.455; COUTO CALVIÑO, R. *Servicios de certificación…op., cit.,* p.40; según la definición recogida en el vigésimo septimo informe sobre comercio electrónico en España a través de entidades de medios de pago, el "TPV virtual se entiende cualquier herramienta software que realiza el envío de las peticiones de pago con tarjeta a las entidades financieras e i dentifica expresamente que la transacción es de Comercio Electrónico (generada desde Internet)", «NOTA Metodológica al informe sobre comercio electrónico en España a través de entidades de medios de pago». Revisión 2007 [En línea] Disponible en Internet: http://www.cmt.es/cmt/centro_info/publicaciones/index.htm (última consulta 2 de mayo de 2012); HERNANDO, Isabel. *Contratos informáticos…op., cit.,* p.478.

[290] ESCOBAR ESPINAR, M. *El comercio…op., cit*., p.171.

ventas realizadas en la red cuando el pago de las mismas es efectuado con tarjeta (crédito o débito)[291].

La pasarela es un software de procesamiento de pagos, puede pertenecer a una entidad financiera (adquirente) o a un operador de medios de pago, el cual procesa las transacciones de un conjunto de entidades[292]. Desempeña la función de mediador, a través de la tarjeta electrónica, en la relación del vendedor con el banco del comprador[293]. Como señala la doctrina, el funcionamiento de la pasarela de pagos o terminal de punto de venta virtual, es el equivalente a una TPV (Terminal de Punto de Venta) física ubicada en la mayoría de los almacenes o establecimientos. Los *gateways* de

[291] SEOANE BALADO, Eloy. *La nueva era...op., cit.,* p.214.

[292] *Comunicación segura a través de redes de información (II*), publicado en marzo de 2000,[En línea] disponible en Internet: http://www.marketingycomercio.com/numero1/1art1pub2000mar_1.htm, (última consulta 2 de junio de 2012).

[293] JAVIER VICENTE BLANCO, D. "Medios electrónicos de pago…"*op., cit.,* pp. 278 y ss; MARTINEZ GÓNZALEZ, M. "Mecanismo de seguridad..."*, op., cit.,* p.10; una de las funciones que desempeña un *gateway* o pasarela de pago es la de facilitar las transferencia de información entre un portal de pago (como ser un sitio web o un servidor) y el banco adquirente de manera rápida y segura. Cuando un cliente ordena un producto de un vendedor que tiene habilitado un *gateway* de pago, el *gateway* de pago realiza una serie de tareas para procesar la transacción, de manera transparente para el comprador. Por ejemplo: -Un cliente realiza un pedido en un sitio web presionando el botón de "emitir orden" o similar o ingresa los detalles de su tarjeta de crédito a un servicio IVR; -Si la orden es a través de un sitio web, el navegador web del cliente cifra la información que viaja hasta el servidor web del vendedor. Esto se hace normalmente mediante cifrado SSL (*Secure Socket Layer*);- El vendedor reenvía los detalles de la transacción a su *gateway* de pago, el cual contiene los detalles de las cuentas de sus vendedores. Normalmente, esta es otra conexión cifra mediante SSL al servidor de pago, almacenada en el *gateway* de pago; -El *gateway* de pago que recibe la información de la transacción del vendedor reenvía la información al banco adquirente del vendedor; -El banco adquirente reenvía la información de la transacción al banco emisor (el banco que le emitió la tarjeta de crédito al cliente) para autorización; -El banco emisor de la tarjeta recibe el pedido de autorización y envía una respuesta al *gateway* de pago (a través del banco adquirente) con un código de respuesta. Además de determinar el destino del pago (es decir, aprobado o rechazado), el código de respuesta se usa para definir la razón por la cual la transacción falló (como por ejemplo, por fondos insuficientes o enlace al banco no disponible); -El *gateway* de pago recibe la respuesta y la reenvía al sitio web (o cualquier otra interfaz que haya sido usada para procesar el pago), donde se interpreta y se releva una respuesta al cliente; El proceso completa demanda unos 3-4 segundos. Al final del período de liquidación, el banco adquirente deposita el total de los fondos aprobados en la cuenta nominada del vendedor. Esta cuenta puede encontrarse en el mismo banco adquirente si el vendedor realiza sus operaciones con el mismo banco o una cuenta con otro banco.

pago cifran información sensible, tal como números de tarjetas de crédito, para garantizar que la información pase en forma segura entre el cliente y el vendedor.

2.5.3.3. *El procedimiento de pago electrónico con SET*

En este punto se describirá el procedimiento en el que se utiliza el protocolo SET para realizar el pago mediante el uso del número de la tarjeta de crédito en Internet.

El proceso de compra o de pago en una transacción electrónica en la que se utiliza la tarjeta de crédito bajo el sistema SET, es el siguiente[294]: el cliente o consumidor, tras seleccionar los productos a comprar en el sitio web del vendedor envía a éste un formulario de pedido que es respondido por el comerciante o proveedor de bienes o servicios con el envío de su certificado digital y el de la pasarela de pago. Una vez que el cliente comprueba la validez de la firma digital o de los certificados, envía al proveedor de bienes o servicios una orden de pago, que está dividida en dos partes[295]:

- ✓ La información sobre el pedido, (*order information*) de la compra, en la que figurarán los datos del producto a comprar y el valor de la misma
- ✓ Las instrucciones de la compra (*payment instruction*), donde se describen los datos bancarios y se dan instrucciones para el pago a la entidad vendedora.

[294] LAFUENTE SÁNCHEZ, R., *Los servicios financieros*…op., cit., p. 242; PLAZA PENADES, J. "Contratación electrónica…"*op., cit.*, pp. 455 y ss; Para comprar con este protocolo se requiere un *software* SET, que es suministrado generalmente por la entidad emisora de la tarjeta, un certificado digital SET y un monedero digital. El certificado digital SET es emitido por la misma entidad emisora de la tarjeta y asegura la legitimidad en el uso de la misma, si se tiene más de una tarjeta electrónica, se requiere un certificado distinto para cada una; igualmente el vendedor necesitará un certificado digital diferente para cada marca de tarjeta que quiera aceptar, el uso de estos certificados proporcionan al comprador la misma seguridad que cuando paga con tarjeta en el establecimiento físico. El monedero digital denominado Wallet, funciona en sentido similar a una cartera física almacenando las diferentes tarjetas electrónicas que posee el comprador y su identificación personal.

[295] ESCOBAR ESPINAR, M. *El comercio…op., cit.*, p.174.

Esta orden de pago se firma digitalmente mediante un algoritmo especial, denominado firma dual[296], en el que se enlazan primero los hash o "resumen" de los dos documentos generados y encriptados, la firma se liga después con la clave pública y seguidamente se encripta la firma doble mediante una clave simétrica generada por el software del cliente. Finalmente, el número de la tarjeta de crédito se cifra con la clave pública del emisor o de la pasarela de pago[297].

De este modo, el proveedor de bienes o servicios no podrá consultar los datos bancarios del cliente. Tampoco el banco puede conocer la información sobre los productos comprados a pesar de que ambos documentos están ligados por la misma firma.

Una vez que el cliente cifra el mensaje, envía el pedido al comprador que, una vez recibida la orden de compra o pedido y la firma dual del cliente, procederá a la verificación de ambas, comprobará su autenticidad, utilizando para ello la firma digital de aquel y su certificado, y la integridad de los datos recibidos. Una vez terminada la comprobación se procede a enviar, a través de Internet, los datos bancarios del cliente a la pasarela de pago, encriptados con la clave pública de la misma.

Como bien indican algunos autores, la pasarela de pago recibe "las transacciones del comercio, verifica los certificados y las firmas del comercio y del titular, descifra la petición de autorización enviada por el comercio y los

[296] El *software* monedero (*wallet*) del cliente genera una firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el el comerciante puede acceder a la información del pedido, pero no a las instrucciones de pago, mientras que el banco puede acceder a las instrucciones de pago, pero no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso, ya que ni el comerciante llega a conocer el número de tarjeta de crédito empleado por el comprador, ni el banco se entera de los hábitos de compra de su cliente; FRAMIÑA SANTA, J. "Pagos en la red...", *op., cit*., p.375.

[297] FRAMIÑA SANTA, J. "Pagos en la red..."*op., cit.,* pp. 375 y ss.

datos de la tarjeta enviados por el titular, con el fin de solicitar la autorización económica del medio de pago que corresponda"[298].

En el caso de que los datos enviados sean correctos, la pasarela de pago envía mediante las redes de comunicación bancarias el *payment instruction* a la entidad emisora o Banco adquirente y solicita autorización para realizar el pago mediante un documento denominado petición de autorización de pago.

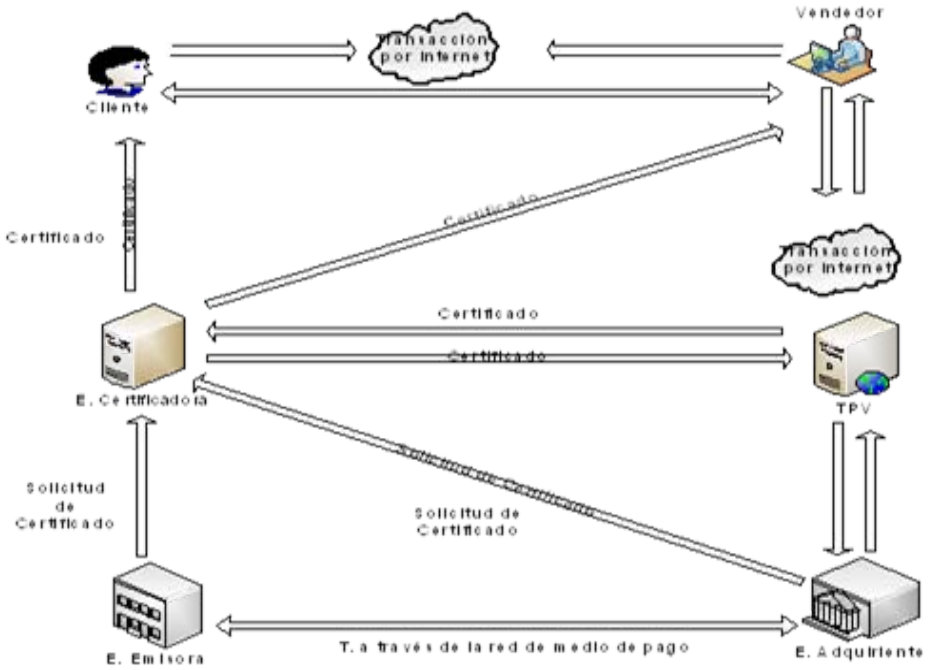
La entidad bancaria comprueba que la tarjeta de crédito es válida y permite el cargo del importe de la compra, enviando entonces un documento a la pasarela de pago, denominado autorización de pago, en el que se autoriza el proceso de compra.

La pasarela de pago notifica el prestador de bienes o servicios la autorización y este último procede al envío de los productos comprados por el cliente, y, después de la entrega física del producto, pide el importe de la venta a la pasarela de pagos, proceso llamado solicitud de pago.

Por último, la pasarela de pago pide al banco del cliente la transferencia del importe de la venta al banco adquirente, petición que recibe el nombre de solicitud de compensación. Por lo tanto, se le hace efectivo al vendedor el importe con lo que se cierra el proceso total de compra. Todos los documentos implicados en el proceso anterior deben llevar un número identificador único de transacción, conocido como ID.

[298] ESCOBAR ESPINAR, M. *El comercio…op., cit*., p. 174.

En la siguiente figura se explica el proceso completo de pago mediante el protocolo o sistema SET. Observen la figura 9.



Fuente: elaborado por el propio autor.

2.5.3.4. *Ventajas e Inconvenientes del SET*

Una de las ventajas que tiene el protocolo SET es que garantiza los siguientes componentes de seguridad:

a) La autenticación: se autentican las partes mediante la emisión de certificados electrónicos, emitidos por un PSC único, lo que impedirá cualquier tipo de usurpación de la identidad así como el uso fraudulento de los datos de la tarjeta de crédito[299].

[299] Vid. LAFUENTE SÁNCHEZ, R. *Los servicios*…op., cit., p. 244; RICO CARRILLO, M. *Comercio electrónico…op., cit.*, p.213; FERNÁNDEZ GÓMEZ, E. *Comercio electrónico…op., cit.,* pp.123 y ss; MADRID PARRA, A. "Seguridad en el*…"op., cit*., p. 165; ESCOBAR ESPINAR, M. *El comercio…op., cit*., p.177.

b) La confidencialidad[300]: permite separar los datos de la tarjeta y los de compra de forma que se transmiten cifrados, por lo que ni el banco ni el vendedor tendrán acceso a ellos. Sólo permite que las partes vean la información que les corresponda. No se puede alterar la información ni duplicarla. Tampoco es posible que el importe u otros campos de las transacciones sean alterados indebidamente.

c) La integridad: los datos (el número de tarjeta de crédito) son firmados digitalmente de modo que se garantiza la integridad de todos ellos, incluso cuando se finaliza la conexión, sin que el vendedor tenga acceso a los mismos[301].

d) El no repudio: basado en el uso de las técnicas de criptografía que hemos comentado en uno de los epígrafes de este trabajo. Según señalan algunos autores, "los mensajes firmados pueden servir de prueba inalterable de que la transacción se produjo de un modo correcto"[302]. Criterio que compartimos porque, una vez que se firma el mensaje, las partes no pueden negar su participación.

A pesar de estas ventajas, el protocolo SET presenta inconvenientes, sobre todo en lo relacionado con problemas técnicos que a su vez conllevan la implantación de estándar de SET, así como problemas prácticos y problemas de naturaleza jurídica.

2.6. Diferencias existente entre el SET y SSL

Las diferencias entre ambos protocolos vienen constituidas por la utilización por parte del protocolo SET de firmas electrónicas en el intercambio

[300] Vid. RICO CARRILLO, M. *Comercio electrónico…op., cit.*, p. 213; FERNÁNDEZ GÓMEZ, Eva. Comercio electrónico…*op., cit.,* p. 124; Gonzalo; ESCOBAR ESPINAR, M. *El comercio…op., cit.*, p.176.
[301] FERNÁNDEZ GÓMEZ, Eva. Comercio electrónico…*op., cit.,* p.124.
[302] RAMOS SUAREZ, F. *Seguridad de...op., cit.,* p. 1.

de información, de manera que se trata de un protocolo que, además de asegurar la integridad de las comunicaciones, tiene la ventaja de autenticar tanto al comprador como al vendedor, lo que evita el repudio de la transacción[303].

Por el contrario, el protocolo SSL no hace uso de firmas electrónicas para la autenticación del cliente; el cliente no necesita autenticarse, por lo que una persona ajena, que no es la titular de la tarjeta, si logra apoderarse del número de tarjeta de crédito de forma ilícita podría realizar cualquier tipo de compra en Internet. Además, el sistema SSL no garantiza la integridad de la información una vez finalizada la conexión, por lo que el vendedor podría modificar esos datos, por ejemplo, cobrando más al cliente[304].

En relación a la confidencialidad en el sistema SET, se garantiza que las partes (el vendedor y el banco) no accedan a los datos del cliente. Si bien el sistema SSL asegura la confidencialidad entre las partes, sin embargo, al finalizar la conexión, el vendedor tiene en su poder todos los datos del cliente, incluyendo el número de tarjeta de crédito. Si el vendedor llegara a almacenar estos datos, el cliente estaría expuesto a cualquier tipo de riesgo, por ejemplo, a que la persona que los tuviera en su poder los manipulara con fines fraudulentos.

Como señala la doctrina, el sistema SET garantiza el no repudio, ya que la firma digital puede servir como prueba de que la transacción ha sido realmente realizada, por lo que las partes intervinientes no pueden negar su participación en ella[305].

Por el contrario, el sistema SSL no garantiza el no repudio y, por lo tanto, una vez finalizada la compra, no existe ningún tipo de comprobante, por lo

[303] MADRID PARRA, A. "Seguridad en el…" *op., cit.,* p.163.
[304] ESCOBAR ESPINAR, M. *El comercio…op., cit*., p.178.
[305] *Ibídem,* pp.177 y ss.

que cualquier protesta posterior carecerá de medios para su confirmación. Tampoco existe documento firmado, por lo que tanto el cliente como el vendedor o el banco podrían negar su participación en la compra sin que existiera la posibilidad de probar lo contrario.

Uno de los problemas que plantea SET es su complejidad con respecto a SSL, ya que requiere que tanto el vendedor como el titular de la tarjeta estén registrados en el sistema SET y que, además, utilicen certificados digitales emitidos por la entidad emisora de la tarjeta que autentique al titular y al banco del proveedor de bienes o servicios (establecimiento) que es donde se realiza el pago[306].

Mientras que en el sistema SSL la autenticación del cliente es opcional[307]. El SET sólo se puede utilizar para el pago con tarjeta de crédito, por el contrario, el SSL es de uso general.

En el SET participa un sujeto intermedio, la pasarela de pagos. En el SSL la interacción se restringe a un úni co cliente (comprador) y un s ervidor (vendedor).

2.7. El protocolo 3DSecure

Es el nuevo sistema de pago desarrollado por Visa y Mastercard con el fin de proporcionar seguridad cuando se realizan compras por Internet y autentificar al comprador, al proveedor de servicios o bi enes y al banco implicado en el pago, utilizando para ello los TPV Virtual disponibles[308]. A este

[306] MADRID PARRA, A. "Seguridad en el comercio*…"op., cit*., p.164.

[307] MARTÍNEZ GONZALEZ, M. "Mecanismo de seguridad…"*op., cit*., p.62; FONT A. *Seguridad*…op., cit., p.66.

[308] SEOANE BALADO, E. *La nueva era...op., cit.,* p. 219; vid. SCHILLACI, Marc. *Como tener éxito con su tienda virtual. Guía práctica de comercio electrónico.* Barcelona: INFORBOOK, S, S.L., 2009, pp. 154 y ss.

sistema se le denomina "Verified by Visa"[309], si la tarjeta del titular es Visa/Visa Electronic y Master Card Secure Code[310], si la tarjeta del cliente es Master Card /Maestro.

El sistema 3D Secure permite verificar la identidad del comprador por medio de una contraseña que el comprador adquiere a través de su banco y que deberá introducir de forma correcta para autorizar la compra. Es una tecnología de autenticación que hace uso del protocolo SSL y un Plug-in al servidor del comercio que informa y verifica los participantes con fines de garantizar la autenticación y confidencialidad de la información durante una compra on líne[311]; es decir, protege la información de pago con la tarjeta durante su transmisión por Internet.

Una de las ventajas que tiene el sistema 3D Secure es que garantiza la seguridad para los clientes en sus compras por Internet. No hace falta la instalación de software especial de aplicaciones en el dispositivo de acceso del cliente.

Este protocolo es fácil de utilizar, sólo se necesita que el cliente posea una clave y una tarjeta Visa para efectuar la compra. En caso de no disponer de la misma, es recomendable que el cliente acuda a su entidad bancaria para solicitar que su tarjeta pueda realizar "pagos seguros" por Internet mediante el sistema Verified by Visa. Es un sistema que agiliza la tramitación del pedido, ya que no es necesario enviar por fax copia del documento de

[309] Verified by Visa es un nuevo servicio que permite a las Instituciones Financieras autenticar la identidad del usuario de la tarjeta durante el proceso de pago de compras en tiendas virtuales.

[310] Master card secure, es un servicio de seguridad en línea para proteger contra el uso no autorizado de su tarjeta Master Card, mientras compra en línea, en los comercios participantes. No requiere la descarga de ningún software, ni existe la necesidad de obtener una nueva tarjeta.

[311] Información [En línea] disponible en Internet: http://www.optize.es(última consulta el 20 de abril de 2012).

identidad, como DNI o NIE y del recibo domiciliado para identificar el titular de la tarjeta.

2.8. Proceso de compra con tarjeta visa mediante 3D Secure

En primer lugar, cuando el cliente elige la forma de pago mediante tarjeta de crédito o débito Visa o MasterCard, se le enlaza con un servidor o página segura que hace uso del protocolo SSL (https://) y el sistema le pedirá sus datos bancarios (número de tarjeta de crédito y fecha de caducidad).

En segundo lugar, cuando se procede a realizar el pago se le abrirá una ventana en la que se le pedirá que teclee su clave personal usada en los cajeros o bien una clave especial que haya solicitado a su banco con anterioridad; además, se le pedirá que introduzca los datos personales como el DNI, NIE o el pasaporte.

En el tercer paso, el cliente verá una página que le indicará el estado de su pago. Si la operación ha sido autorizada por el banco, se le facilitará el código de autorización. Puede imprimir esta página. Debe presionar el botón "Cerrar" para finalizar el proceso de compra.

Por último, cabe señalar que las tecnologías Verified by Visa o MasterCard Secure Code crean contraseñas para las tarjetas del usuario. Una vez finalizado el proceso de creación de la clave, el usuario podrá únicamente realizar la compra introduciendo dicha clave. Permite solucionar algunos inconvenientes de SSL, como la posibilidad de que el comerciante o proveedor de bienes o servicios utilice la tarjeta del cliente en futuras compras.

2.9. La seguridad jurídica en la operativa de pago mediante tarjeta de crédito o débito en el comercio electrónico

Una vez que hemos analizado la seguridad desde el punto de vista técnico, nos gustaría acometer el análisis sobre las cuestiones relacionadas con la seguridad jurídica en las transacciones electrónicas. Cabe reseñar que la esencia de la seguridad jurídica en el comercio electrónico va más allá de la garantía de la integridad y seguridad de las comunicaciones. Es decir, uno de los aspectos básicos de la seguridad jurídica en el sistema de pago electrónico se relaciona con la definición de las obligaciones de los sujetos intervinientes en la transacción, con el fin de determinar la atribución de la responsabilidad ante el incumplimiento de las obligaciones y cargas que corresponden a cada uno de ellos y los posibles fallos que puedan originarse en la transacción[312].

En este sentido, la Ley 22/2007, sobre comercialización a distancia de servicios financieros destinados a los consumidores, en su art. 9.1 LCDSFC establece la obligación de las entidades de comunicar al consumidor todas las condiciones contractuales, así como la información contemplada en los anteriores artículos 7 y 8, en soporte de papel u otro soporte duradero accesible al consumidor, con suficiente antelación a la posible celebración del contrato a distancia o a la aceptación de una oferta y, en todo caso, antes de que el consumidor asuma las obligaciones mediante cualquier contrato a distancia u oferta.

[312] Siguiendo a RICO CARRILLO, M.: quien sostiene que "la seguridad jurídica se refiere a la protección que otorga al derecho, la cual se encuentra delimitado en normas de orden legal…"en esta misma línea, este autor sostiene que "en el ámbito jurídico, la protección de las transacciones electrónicas se lleva a cabo mediante el respeto de los derechos de los consumidores y la determinación de la responsabilidad de cada uno de los sujetos que intervienen en la transacción", en RICO CARRILLO, M.: "Responsabilidad civil de los intermediarios derivada del pago con tarjetas en el comercio electrónico a través de Internet», en *Revista de Derecho Informático*, núm. 017 diciembre del 1999, pp1-10, en especial p.1. [En línea] disponible en Internet: http://vlex.com/vid/intermediarios-derivada-tarjetas-internnet-107444(última consulta 3 de marzo de 2012).

También se añade en el precepto 10.1 LCDSFC el derecho de desistimiento. "El consumidor dispondrá de un plazo de catorce días naturales para desistir del contrato a distancia, sin indicación de los motivos y sin penalización alguna".

Por su parte, el art. 106 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU), prevé la garantía para los consumidores y usuarios de la tarjeta, tras establecer que el titular de la tarjeta cuyo número ha sido utilizado indebida o fraudulentamente por un tercero tiene derecho a anular el cargo fraudulento.

Asimismo, la Ley 59/2003, de firma electrónica, resulta ser un instrumento imprescindible para reforzar la confianza de los sujetos intervinientes en las transacciones electrónicas ya que facilita la comprobación de la procedencia e integridad de las informaciones intercambiadas a través de Internet para garantizar la seguridad jurídica.

Desde el punto de vista de la seguridad jurídica en la operativa de pago mediante tarjeta de crédito o débito en el comercio electrónico, la Ley 16/2009, de 13 de noviembre, de servicios de pago, garantiza un alto nivel de protección gracias a la definición y el establecimiento de los derechos, obligaciones y responsabilidad de los usuarios y de los proveedores de servicios de pago, previstos en el Titulo IV, Capítulo II y Capítulo III, Sección III.

Por último, se ha de concluir que la seguridad jurídica[313] en relación con el derecho del comercio electrónico supone la existencia de mecanismos, de

[313] Véanse, PECES-BARBA, Gregorio. *Curso de derechos fundamentales,* vol. I. Madrid: Eudema, 1991, pp. 214-215; LEGAZ LACAMBRA, Luis. *Filosofía del Derecho*. 2. ª ed. Madrid: 1961; GUASP, Jaime*. Derecho.* Madrid: Edit. Ergos, 1971; BERMEJO VERA, José.

técnicas, formuladas como principios de organización, de interpretación o como derechos subjetivos que funcionan en el interior del ordenamiento.

2.10. Consideraciones finales

Teniendo en cuenta los diversos trabajos de investigación existentes en la materia hemos visto como uno de los principales problemas que enfrenta el pago con tarjeta en el comercio electrónico a través de Internet en la actualidad es todo lo relacionado con la seguridad.

Así pues, a modo de conclusión, cabe señalar que la seguridad en las transacciones electrónicas u operaciones en las que se hace uso del número de la tarjeta electrónica (de crédito o débito), viene siendo una de las cuestiones fundamentales para el desarrollo del comercio electrónico. Sobre todo, la falta de presencia física simultánea de las partes contratantes en el comercio electrónico se convierte en uno de los factores que genera desconfianza e inseguridad entre los entes intervinientes en el contrato de cambio realizado en el comercio electrónico.

En este sentido, somos de la opinión de que, para minimizar el nivel de inseguridad o desconfianza de los usuarios en los medios de pago electrónico, es necesario garantizar la seguridad, tanto técnica como jurídica en el comercio electrónico, para así evitar o prevenir el uso indebido o fraudulento de la tarjeta en aquellas operaciones llevadas a cabo en Internet.

Desde el punto de vista técnico, los componentes o mecanismos de seguridad en las transacciones electrónicas, como, por ejemplo, la autenticación, integridad, confidencialidad y el no repudio, tanto de origen como destino, son fundamentales para dar confianza a la hora de realizar pagos en el comercio electrónico.

El declive de la seguridad en el ordenamiento plural. Cizur Menor (Navarra): Aranzadi, SA, 2005, pp. 39 y ss.

En fin, cabe subrayar que los mecanismos básicos para hacer cumplir dichos componentes o requisitos de seguridad mencionados con anterioridad son:

- las técnicas criptográficas (asimétrica o simétricas);
- la firma electrónica
- los certificados electrónicos

Todos ellos desempeñan un papel de especial importancia en la protección técnica de los datos y constituyen un factor esencial en el desarrollo del comercio electrónico; o sea, estas tecnologías seguras, basada en métodos criptográficos, promueven la confianza financiera a través de la seguridad de los pagos electrónicos.

Se ha de reseñar que, a los mecanismos de seguridad a que nos hemos referido en a lo largo del presente trabajo, se suman los protocolos de seguridad, tales como:

- SSL (Secure Sockets Layer)
- SET(Secure electronic Transaction)
- 3 D Secure,

Todos estos son protocolos desarrollados por distintas empresas o entidades emisoras de medios de pago electrónico que desempeñan una función primordial en las transacciones electrónicas.

Como hemos señalado a lo largo de este trabajo, una de las funciones del protocolo SSL es cifrar la información intercambiada en Internet entre el ordenador del cliente y el propio servidor del proveedor de bienes o servicios, utilizando conjuntamente cifrados simétricos y asimétricos con el objetivo de impedir que un tercero no autorizado pueda tener acceso a los datos.

Además, este sistema permite la autenticación y privacidad de la información entre extremos en Internet mediante el uso de criptografía.

Asimismo, cabe señalar que este protocolo sólo garantiza la autenticación del servidor (vendedor); es decir, garantiza su identidad mientras que el cliente se mantiene sin autenticar(es opcional), situación que puede traer consigo que una persona ajena que se apodere del número de tarjeta y los datos personales del titular pueda realizar transacciones en Internet.

Por último, siguiendo las tesis sostenidas por la doctrina, hemos de resaltar que el protocolo SSL no permite ir más allá de la autenticación y seguridad de la comunicación ya que no permite comprobar si el cliente está autorizado a pagar con tarjeta o no, ni el tipo de pago que tanto cliente como comerciante pueden realizar, ni otras informaciones similares; o sea este tipo de sistema carece de capacidad para verificar la validez del número de tarjeta recibido y autorizar la transacción con la entidad emisora de la tarjeta. Por lo que deja abierto el camino para posible fraudes como la compra con tarjetas robadas o el repudio; lo único que hace es asegurar la interacción entre comprador y vendedor cuando los datos viajan desde el navegador hasta el servidor.

En esta línea, es importante señalar que el protocolo SET surge a raíz de los inconvenientes que presenta el sistema SSL, en todo lo relacionado con la autenticación y el no repudio ya sea de origen o destino. Por otra parte, referido al sistema SET, cabe señalar que uno de los objetivos que tiene dicho protocolo es la de garantizar la autenticación de todas las partes que intervienen en la transacción cuando se utilizan las tarjetas de crédito o de débito como medios de pago en Internet; también garantiza la integridad de la información intercambiada (como el número de tarjeta, que no podrá ser alterada de manera accidental o maliciosa durante su transporte a través de

redes telemáticas). Para lograrlo, el mensaje se cifra y se firma sin que la otra parte tenga acceso a los datos y a la confidencialidad de la información; es decir, permite garantizar la seguridad del pago en Internet. Para ello, se utiliza el sistema asimétrico o de clave pública, firma digital y certificado electrónico.

Una de las ventajas que conlleva este tipo de protocolo es que garantiza la autenticación, confidencialidad, integridad y no repudio. Sin embargo, presenta algunos inconvenientes, como es el de que su implantación se haya visto frenada, siendo muy poco utilizado en la actualidad.

Teniendo en cuenta los inconvenientes que presenta el sistema SSL, se ha de plantear la necesidad de la creación de un nuevo sistema de seguridad para el comercio electrónico, con la finalidad de garantizar la seguridad y así poder evitar el fraude en las transacciones electrónicas llevadas a cabo en Internet. Ya que dichos inconvenientes lo convierten en un protocolo de seguridad deficiente desde el punto de vista del pago electrónico mediante el uso del número de la tarjeta de crédito o débito en el comercio electrónico. Lo cierto, es que la implantación de un nuevo protocolo de seguridad en el comercio electrónico requiere de un gran esfuerzo y compromiso por parte de las entidades bancarias y empresas que lo utilicen porque no se puede seguir intentando dar soluciones a los fraudes con un protocolo que no está diseñado para tal fin.

Por último, cabe señalar que el uso de los métodos criptográficos, firma digital y certificado electrónico, no son suficientes para conseguir un elevado nivel de seguridad en el comercio electrónico. Es decir, el avance del comercio electrónico no depende sólo de la seguridad técnica sino también de la seguridad jurídica. Por lo tanto, la seguridad jurídica juega un papel fundamental en el desarrollo del comercio electrónico.

Lo cierto es que, desde el punto de vista jurídico, existía cierta inseguridad con respeto al pago electrónico, propiciada sobre todo por la no existencia de una normativa jurídica específica que regulase lo relacionado con los servicios de pago electrónico en el derecho español. Sin embargo, con la promulgación de la Ley 16/2009, de 13 de noviembre, de servicios de pago, que traspone al ordenamiento interno la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, de servicios de pago en el mercado interior, se establece, en su Título IV, capítulo II, arts. 27 a 31 y art. 45, un sistema común de derechos y obligaciones para proveedores y para usuarios en relación con la prestación y utilización de los servicios de pago.

Al mismo tiempo, el legislador español con el fin de proteger a los consumidores y usuarios que celebran el contrato de cambio en el comercio electrónico aprueba las siguientes normativas: el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU); la Ley 22/2007, sobre comercialización a distancia de servicios financieros destinados a los consumidores(LCDSFC); y la Ley 47/2002, de 19 de diciembre, de Reforma de la Ley de Ordenación del Comercio Minorista, para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE, en materia de contratos a distancia y para la adaptación de la ley a diversas directivas comunitarias.

Universidad Carlos III de Madrid

CAPÍTULO TERCERO

RELACIONES JURIDICAS PARA EL PAGO ELECTRÓNICO CON TARJETA

CAPÍTULO. III

RELACIONES JURIDICAS PARA EL PAGO ELECTRÓNICA CON TARJETA

3. Precisiones introductorias

Una vez analizadas las distintas concepciones de la doctrina y la jurisprudencia española así como el derecho comparado sobre el concepto de tarjeta de pago y los sujetos intervinientes, y habiendo fijado nuestra postura con respecto a la misma, creemos que es necesario estudiar las distintas relaciones contractuales que vinculan a los entes intervinientes en las operaciones electrónicas de pago mediante tarjeta.

Hemos de señalar que el contrato de tarjeta electrónica de pago es el tipo contractual base en el que se comprenden tres tipos de contratos específicos: el contrato de cuenta de crédito mediante tarjeta, el contrato de tarjeta de compra y el contrato de tarjeta de débito[314]. Entre estas figuras contractuales mencionadas, optaremos por estudiar la del contrato de cuenta de crédito mediante tarjeta, o sea, el contrato de tarjeta de crédito.

De hecho, las interacciones entre los sujetos intervinientes en el contrato de tarjeta electrónica de pago, así como la utilización de la misma en todas sus modalidades técnicas y operativas, implican una estructura subjetiva o una serie de vínculos o relaciones jurídicas complejas y plurilaterales[315]. Por

[314] GETE-ALONSO y CALERA, M.C. *El pago mediante*…, op., cit., p. 34.

[315] En este mismo sentido, la SAP de Madrid de 11 de abril de 1987, califica la relación jurídica que genera el contrato de tarjeta de crédito, de "plurimembre y compleja", es decir da lugar a diferentes contratos; vid. RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo…"*op., cit.,* pp. 319-371; BARUTEL MANAUT, C, *Las tarjetas de…*op., cit., pp. 102-149; GÓMEZ PORRÚA, J. M. "La tarjeta...", *op., cit*., pp.193 y ss; PEREZ-SERRABONA, J.L. y FERNÁNDEZ, J.M. *La tarjeta de…op., cit.;* GETE-ALONSO y CALERA, M. C. *El pago mediante...op., cit.,* p.35; COLLS, M. *El dinero de plástico. Todo sobre las tarjetas de*

ejemplo, la relación entre la entidad emisora de la tarjeta y el titular de la misma, entre la entidad emisora o el banco adquirente y el proveedor de bienes o servicios adherido al sistema[316], y, como consecuencia de estas dos relaciones contractuales, surge una tercera relación entre el titular de la tarjeta y el proveedor de los bienes o servicios (establecimiento comercial) adherido al sistema.

Además, pueden surgir nuevas relaciones contractuales que son ajenas a la relación contractual propia del contrato de tarjeta de pago en las que interviene un intermediario como, por ejemplo, el proveedor de acceso a la red, con quien se contrata la conexión a Internet. Pues bien, puede existir el vínculo contractual entre el proveedor de acceso con el titular de la tarjeta, el mismo proveedor de acceso con el proveedor de bienes o servicios, y éste con la entidad emisora de la tarjeta; además, puede existir otra relación con los proveedores de servicios de certificación.

Teniendo en cuenta lo planteado con anterioridad sobre la relación existente entre las partes intervinientes en el contrato de tarjeta de crédito, nos interesa examinar en este capítulo el contrato de emisión de la tarjeta, el contrato de aceptación de la tarjeta y el contrato de acceso a Internet, que conforman el contrato de tarjeta de crédito, sus contenidos y alcances, con el fin de determinar las responsabilidades de cada uno de los entes participantes en la emisión y utilización de la tarjeta de pago electrónico.

---

crédito. Barcelona: Decálogo, 1990, 47 p; JAVIER VICENTE BLANCO, D.: "*Medios Electrónicos*…"*op., cit.,* pp. 278 y ss; BATUECAS CALETERIO, A*. Tarjeta de crédito*…*op., cit.* pp.185 y ss; MARIÑO LÓPEZ, Andrés. *Uso fraudulento de tarjetas crédito por terceros no autorizados. Daños y responsabilidad civil.* Madrid: Marcial Pons, 2006, p.18; GÓMEZ MENDOZA, M. "Tarjeta*…"op., cit.,* p.378; ARIAS POU, M. ª *Manual práctico de... op., cit*., p.455; a favor de este criterio LAFUENTE SÁNCHEZ, R.: *Los servicios financieros*…, *op., cit.,* p.246; RIVERO ALEMÁN, S. *Crédito, Consumo y…, op., cit.,* p. 544.

[316] Sin embargo, puede aparecer una figura llamada entidad adquirente, es decir, esto ocurre cuando la figura de la entidad emisora, no coincide con el banco o entidad adquirente, que celebra acuerdos con el proveedor de los bienes o servicios (establecimiento comercial) para la futura aceptación de la tarjeta.

También y de manera breve definiremos en qué consiste el contrato de acceso o conexión a Internet.

Por último, a lo largo de este capítulo desarrollaremos un epígrafe basado en las obligaciones de los sujetos intervinientes en los distintos contratos mencionados con anterioridad, así como las obligaciones que corresponden a los proveedores de acceso a Internet y prestadores de servicios de certificación que emiten certificados electrónicos; todo ello en caso de que la operativa de pago se lleve a cabo mediante el protocolo SET.

3.1. El contrato de emisión de la tarjeta

3.1.1. Concepto

La relación jurídica contractual existente entre el emisor y el titular de la tarjeta es compleja y sus condiciones se estipulan en un documento denominado "contrato de emisión de tarjeta"[317]. Como indica la doctrina, el contrato de emisión de tarjeta "es aquel contrato que va posibilitar al emisor realizar delegaciones de deuda". Sin embargo, "la celebración de dicho contrato no persigue practicar una delegación de deuda en ese mismo instante, sino que su fin principal consiste en posibilitar que puedan materializarse delegaciones futuras de deudas cada vez que el titular de la tarjeta utilice la tarjeta"[318].

[317] BARUTEL MANAUT, C. *Las Tarjetas de…o., cit.,* p. 303; BATUECAS CALETRIO, Alfredo. *Pago con tarjeta de crédito. Naturaleza y régimen jurídico. Revista Aranzadi de Derecho Patrimonial,* núm. 15. Navarra: 2005, p.186 y ss; vid. GETE-ALONSO y CALERA, M.C.: *El pago mediante...op., cit.,* p. 34, sostiene que se trata de una "relación contractual básica y fundamental en el esquema global y complejo; RIVERO ALEMÁN, S. *Crédito, Consumo y…op., cit.,* p. 545.

[318] En este sentido BATUECAS CALETRÍO, pone de relieve que "con este acuerdo se crea el marco legal apropiado que permite a las partes realizar delegaciones de deuda en un tiempo posterior. precisamente, en la circunstancia futurible reside la razón de la validez de este acuerdo interno materializado entre el titular de la tarjeta y la entidad de crédito. Al no estar celebrándose en este momento una delegación de deuda, sino, simplemente, estableciéndose las bases para su ejecución futura, no es necesaria la presencia del consentimiento del establecimiento comercial (presencia requerida obligatoriamente por el

Con la firma de este contrato, el emisor otorga al titular de la tarjeta la facultad de disfrutar de diversos servicios, principalmente financieros, comprometiéndose a pagar, por cuenta del titular, los bienes o servicios que éste adquiera, mediante la utilización de la tarjeta de pago, en los establecimientos del propio emisor o en aquellos establecimientos adheridos al sistema, o extraer dinero en cajeros automáticos (para lo que se le facilita un número clave, personal y secreto)[319] y, en su caso, la utilización del número de tarjeta en el comercio electrónico.

En este sentido, hay quien define el contrato de emisión de la tarjeta como «aquél en que una persona (la entidad emisora o gestora de la tarjeta) se obliga, frente al titular de la tarjeta, a pagar las obligaciones que éste contraiga con determinadas personas y/o a facilitar dinero en efectivo y otros servicios de caja, a crédito (tarjeta de crédito y de débito) o aplicar ciertas reglas en el pago de las obligaciones de dinero (tarjeta de compra), siempre que aquél haya utilizado la tarjeta que facilita el propio emisor o gestor; y el titular de la tarjeta se obliga a reembolsar las cantidades pagadas por aquél, y en su caso, los intereses y demás gastos y la cuota por su utilización, y a usar la tarjeta de acuerdo con lo estipulado en el contrato»[320].

3.1.2. Caracteres jurídicos del contrato

Podemos calificar el contrato de emisión de la tarjeta como un «contrato atípico»[321], puesto que no está sujeto a regulación legal específica. También

art. 1205 CC). Dicho consentimiento será necesario en el momento en que vaya a celebrarse cada operación de delegación en concreto", en BATUECAS CALETRÍO, A. *Pago con...op.*, cit., pp.186 y ss, nota al pie núm.1.

[319] FERNÁNDEZ LÓPEZ, Juan Manuel. "Tarjetas bancarias", *Contratos bancario y financieros. Cuadernos de Derecho Judicial.* Madrid: Consejo General de Poder Judicial, 1993, pp. 202 y ss.

[320] GETE-ALONSO y CALERA, M.C. *El pago mediante*…op., cit., p. 34; DAVARA RODRÍGUEZ, M. *Manual de Derecho…*op., cit., p. 315.

[321] GETE-ALONSO CALERA, M.C. *El pago mediante*…op., cit., pp. 26- 27 éste señala en uno de sus obras que "el contrato de emisión es un contrato atípico por el hecho de no tener una regulación específica propia, sin embargo, tiene lugar a través del principio de la

se puede considerar como un contrato-tipo, en el que el emisor no negocia individualmente sino que contrata en masa[322]. Pues lo que hace es repetir uniformemente una serie de contratos iguales en los que preestablece unas condiciones generales iguales para todos los titulares; lo único que varía son las condiciones particulares de límite de crédito y disposiciones, tipos de tarjetas y servicios accesibles, además de los sistemas de pago disponibles.

El contrato de emisión es un contrato de adhesión[323], en el que las cláusulas son fijadas unilateralmente por el emisor, limitándose el titular a aceptarlo o rechazarlo en bloque. Es decir, la persona contratante no está en posición de discutir las condiciones contractuales, sino que se limita únicamente a aceptarlas o rechazarlas.

En la doctrina Italiana[324], hay quien lo define como «aquel en que las cláusulas son dispuestas por uno de los futuros contratantes de manera que el otro no puede modificarlas ni puede hacer otra cosa que aceptarlas o rechazarlas, de tal suerte que este último no presta colaboración alguna a la formación del contenido contractual, quedando así sustituida la ordinaria

autonomía de la voluntad contractual (art. 1225 CC)"; vid. FERNÁNDEZ LÓPEZ, J. M. "Tarjetas…"*op., cit*., p. 203; según señala la SAP de Alicante(Secc. 9ª), de 30 de marzo de 27, "son considerados por la doctrina, contratos atípicos por cuanto no tienen una regulación legal especifica, de ahí la importancia que para su regulación tiene la voluntad de las partes(art. 1255 del CC), pero tampoco podemos olvidar que como contrato bancario que son, tienen la condición de contratos de adhesión cuyas cláusulas son impuestas por una entidad bancaria, que las remite al cliente quien las suscribe de forma global, sin negociación ninguna, por lo que cualquier caso la interpretación de su contenido deberá en cualquier caso, acogerse a la Ley 26/1984, General para la Defensa de los Consumidores y Usuarios". Actualmente esta Ley que refiere la SAP de Alicante, fue sustituida por el Real Decreto Legislativo 1/2007, Ley General para la Defensa de los Consumidores y Usuarios, que será estudiada en el capítulo IV de este trabajo; vid. GUIMARÃES, M. R. "El pago mediante…"*op., cit.,* p. 174.

[322] BARUTEL MANAUT, C. *Las tarjetas de…op., cit*., p. 304; GÓMEZ PRÚA, J.M. "La tarjeta de crédito…"*op., cit.,* p. 193.

[323] BARUTEL MANAUT, C. *Las tarjetas de…*op., cit., p. 304; PÉREZ-SERRABONA GONZÁLEZ, J. L.; y FERNÁNDEZ FERNÁNDEZ, L. M. *La tarjeta de…op., cit.,* pp. 57 y ss; GÓMEZ PRÚA, J. "La tarjeta de…"*op., cit.,* p. 194; GETE-ALONSO y CALERA, M.C. *El pago mediante…*op., cit., pp. 34 y ss.

[324] MISSINEO, Francesco*. Il contratto in genere*. Milano: Editorial Giuffrè, 1973, 486 p, Citado por S. STIGLITZ, Rubén y A. STIGLITZ, Gabriel. *Contratos por adhesión, clausulas abusivas y protección al consumidor.* Buenos Aires: Depalma, 1985, p. 50.

determinación bilateral del contenido del vínculo por un simple acto de aceptación o adhesión al esquema predeterminado unilateralmente»[325].

El contrato de adhesión está integrado por cláusulas que se denominan condiciones generales, cuyas notas más sobresalientes responden a la circunstancia de ser redactadas exclusiva e íntegramente por una parte que adopta el nombre de predisponente (entidad bancaria).

Para algunos autores, las condiciones generales se pueden definir como «los conjuntos de reglas que un particular (empresario, grupo o rama de industriales o comerciantes) ha establecido para fijar el contenido (derecho y obligaciones) de los contratos que sobre un determinado tipo de prestaciones se propone realizar»[326]. En esta misma línea, el art.1 LCGC prevé "que las condiciones generales son regulación destinada a disciplinar uniformemente la relación contractual del contrato de adhesión"[327].

Este contrato se caracteriza porque en él las partes que contratan ya no elaboran conjunta y equitativamente los contenidos del acuerdo de voluntades. En muchas ocasiones, en estos contratos se presentan circunstancias en las que el predisponente abusa de su condición jurídica e incluye cláusulas que le benefician y que gravan injustificadamente a su co-contratante, lo que genera un efecto de desequilibrio contractual.

Se trata de un contrato sinalagmático o bilateral, del que nacen derechos y obligaciones de las partes. Es un contrato *intuitu personae*, en el que el emisor tiene en cuenta la solvencia económica y moral del futuro titular a la hora de contratar; no se transmite a los herederos y es intransferible. Pueden concurrir varios titulares complementarios que asumen

[325] CASTAN TOBEÑAS, J. *Derecho civil español, común y foral,* t. III. Madrid: Ed. Reus, 1978, p. 419.

[326] DE CASTRO y BRAVO, F. « Las condiciones generales de los contratos y la eficacia de las leyes», *ADC,* 1961, p. 297.

[327] España: Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación (*BOE,* núm. 89, de 14 de abril de 1998).

solidariamente las obligaciones con el titular contratante, por lo que estaríamos ante una relación multilateral[328].

Es un contrato normativo o contrato marco, ya que regula las posibles relaciones jurídicas-económicas entre las partes o con terceros. Es un contrato oneroso, porque, como contraprestación al servicio que le presta, el titular paga al emisor una serie de comisiones o cánones por la utilización, e intereses en el caso de que se le conceda crédito.

Puesto que está destinado a cumplirse en el tiempo es un contrato de ejecución continuada, es decir, a partir del momento en que se perfecciona su complejo entramado de derechos y obligaciones se ejecutan continuamente, con un plazo de duración indefinido.

Desde otro punto de vista, es un contrato complejo o mixto[329] porque reúne elementos de varios negocios jurídicos. Como, por ejemplo, del contrato de arrendamiento de servicios, del contrato de apertura de crédito y del contrato de cuenta corriente mercantil y bancaria. Por último, diremos que es un contrato consensual que se perfecciona por el consentimiento de las partes formulado por escrito y con la entrega y recepción de la tarjeta.

Respecto a la posición adoptada por las sentencias de los tribunales españoles que han abordado cuestiones relacionados con el contrato de emisión de tarjeta, cabe citar la STS (Sala 2ª.) de 22 de noviembre de 1976, en la que se califica el contrato de emisión de tarjeta como contrato de préstamo, «por el que un banco concede a un particular un préstamo, de numerario, en el que no se fija la cantidad prestada, sino un límite máximo

[328] BARUTEL MANAUT, C. *Las tarjetas de…op., cit*., p. 305.

[329] INFANTE PÉREZ, V. *Tarjeta de*…op., cit p. 34; BARUTEL MANAUT, C. Las tarjetas de…op., cit., pp. 303 y ss; a juicio de SÁNCHEZ CALERO, F. *Instituciones de Derecho Mercantil.*vol II, 24 ed. Madrid: MacGraw-Hill, 2002, p. 330. Se trata de "un contrato de tarjeta de crédito mixto, porque funde --bajo una causa única-- elementos de diversos contratos, como el de comisión, el de arrendamiento de servicios y, eventualmente, el de apertura de crédito".

que no puede sobrepasar el prestatario, y sin que las sumas en cuestión sean entregadas directamente a éste, comprometiendo simplemente el banco a satisfacer a los vendedores el importe de las adquisiciones mobiliarias que realice el titular de la tarjeta y que no exceda del límite señalado, debiendo rembolsar más tarde el prestatario al banco las cantidades satisfechas por cuenta de aquél más los intereses o prestaciones complementarias convenidas, realizando el titular la adquisiciones mentadas, mediante la presentación de la tarjeta y suscripción o aceptación de las oportunas facturas, cuyo importe perciben los vendedores presentándolas al banco expedidor de la tarjeta».

En cambio, la mayoría de la doctrina, a la que nos adherimos, plantea que resulta errónea o inadmisible la tesis sostenida por el Tribunal Supremo[330]. Lo que sí parece evidente, desde nuestro punto de vista, es que el contrato de préstamo no se define por la obligación de entregar sino por la entrega de la cosa; se trata de un contrato real y unilateral que sólo produce obligaciones para el prestatario. En el préstamo existe una sola obligación que es la de devolver el dinero del que se ha dispuesto y el pago de intereses.

Por otra parte, la SAP de Valencia (Sección.2ª.) de 10 de octubre de 1994, indica que se trata de un contrato único en el que se «atribuye al cliente un derecho de crédito diario hasta el límite que fije el banco y global hasta el crédito total».

[330] En contra de la tesis sostenida por el Tribunal Supremo, DE ARRILLAGA, J. I. «La tarjeta de…» op., cit., p. 789; en la misma línea, calificándola como contrato de apertura de crédito, GÓMEZ MENDOZA, "Tarjetas...", *op., cit.*, pp. 380 y 381; GÓMEZ PORRUA, «La tarjeta de crédito», *op., cit.,* p. 692; BARUTEL MANAUT, siguiendo el criterio de éste autor, "no se puede considerar la relación existente entre emisor y el titular como préstamo. Y según se prevé en el art. 1.740 CC, el préstamo consiste en la entrega por una de las partes (prestamista) a la otra (prestatario) de alguna cosa no fungible para que se la devuelva", en BARUTEL MANAUT, C. *Las tarjetas de*…op., cit., pp. 308 y ss.

En la contratación que nos ocupa es usual que los proveedores establezcan el vínculo contractual sobre la base de contratos pre impresos, que contienen cláusulas generales y especiales sin posibilidad para el cliente de discutirlas. Esta situación puede llevar muchas veces al abuso, "muy especialmente cuando el empresario aprovecha de su dominio negocial para exonerarse de responsabilidades o limitar sus consecuencias, para atenuar sus obligaciones o facilitar la ejecución a su cargo, o, desde la perspectiva del consumidor, para agravar subrayadamente sus cargas, acentuar sus deberes, establecerle plazos estrangulantes, invertir en su contra la carga probatoria; en fin, desequilibrar el principio de reciprocidad de las estipulaciones, de tal suerte de acumular ventajas en su favor y simultáneamente desventajas en las prestaciones del cliente"[331].

Finalmente, debe destacarse que los contratos celebrados en el ámbito del comercio electrónico, en cumplimiento de los cuales se pueden utilizar las tarjetas (crédito o débito), son también en la práctica y generalmente contratos redactados de manera previa y unilateral por el comerciante o prestador de servicios «on line», sin que su cliente tenga la posibilidad de negociar los términos de los mismos[332]. Es precisamente en este contrato de emisión de tarjeta donde se contemplan los deberes, derechos, obligaciones y cargas, tanto del emisor como del titular, que examinaremos a lo largo de este capítulo.

[331] S. STIGLITZ, R; y A. STIGLITZ, G. *Contratos por adhesión, cláusulas abusivas y protección al consumidor.* Buenos Aires: Depalma, 1985, p. 95.

[332] Siguiéndonos el criterio sostenido por GUIMARÃES, la cláusulas de estos contratos aparecen en el sitio web donde se ofrecen productos, limitando el cliente al presionar una tecla de su ordenador, correspondiendo a un campo previamente seleccionado en la pantalla, donde se declara éste que, la mayor parte de las veces, ni se quiera se ha llegado a conocer. GUIMARÃES, M. R."El pago mediante…"*op., cit.,* pp. 174 y ss; vid. BARRIUSO RUIZ, C. *La contratación…op., cit.,* pp. 236 y ss; vid. GUISADO MORENO, Á. "Formación y…"*op., cit*., pp. 185 y ss; vid. DOMÍNGUEZ DUELMO, A. "La contratación…*op., cit*., pp. 88 y ss.

3.2. Tipos de contratos relacionados con el contrato de emisión de tarjeta

3.2.1. Contrato de apertura de crédito mediante tarjeta

En efecto, para que la tarjeta funcione, es necesario que la entidad emisora celebre con el futuro titular de la tarjeta un contrato de apertura de crédito, de acuerdo al cual la entidad bancaria asegura al cliente que dispondrá de una suma de dinero, cuando lo requiera, en la forma y condiciones que se estipulan.

La doctrina mayoritaria española que ha estudiado detenidamente el contrato de emisión de tarjeta encuadra dicho contrato en el tipo contractual básico de apertura de crédito[333] en el que se califica la relación jurídica entre el titular y el emisor de contrato de apertura de crédito. Para esta doctrina la relación jurídica se asemeja a la derivada de un contrato de apertura de crédito por el que el emisor se compromete a pagar, por cuenta del titular, los bienes o servicios que éste adquiera, mediante el uso de la tarjeta.

Hay quienes señalan que «no es que se niegue la apertura de crédito en el contrato de emisión de tarjeta, la cuestión está en que sólo se puede acentuar esta relación en determinados casos, y lo que se considera interesante es encontrar aquella relación jurídica que más se asemeja al entramado contrato básico y que pueda albergar, subsumidas en ella, otras relaciones jurídicas permanentes u ocasionadas, como abrir crédito»[334].

[333] Los autores que siguen esta línea explican la relación básica de los contratos de emisión de tarjeta, ARRILLAGA, J. I., «La apertura de crédito», *Revista de Derecho Privado*, núm. 65, Madrid, 1981, pp. 784-804; GÓMEZ DE MENDOZA, M. "Tarjetas…", *op., cit.,* p 381; GÓMEZ PRÚA, J. "La tarjeta", *op., cit.,* p. 189; LÓPEZ RICO, E. J. Tarjeta de crédito: su estudio jurídico, cit., p. 53; DAVARA RODRÍGUEZ, M. *Derecho*...op., cit., pp. 286-292; en contra de esta tesis, GETE-ALONSO CALERO, M.C. *El pago...*op., cit.,..; MARTINEZ-CAÑABATE, Javier R., «El contrato de emisión de tarjeta de crédito bancaria», en *Revista General del Derecho,* núm. 567, Madrid, diciembre de 1991.

[334] BARUTEL MANAUT C. *La tarjeta*…op., cit., p. 312.

Tratándose de una apertura de crédito vinculada a tarjetas de crédito, la entidad emisora se obliga a poner a disposición del usuario el dinero necesario para hacer los pagos de compras y servicios que contrate con la tarjeta. Es decir, el emisor abre un crédito para que el usuario pueda comprar en Internet sin tener que pagar en efectivo y se obliga, también, a pagar las adquisiciones que el usuario haya realizado.

Además, frente al proveedor de bienes o servicios (comerciante) adherido al sistema, el emisor se compromete a pagarle las compras efectuadas con tarjeta. El crédito será utilizable por el usuario mediante un sistema de compras o de adquisición de servicios en determinados comercios, en las condiciones convenidas y en la forma que se reglamenta en el contrato normativo.

Cuando el usuario efectúa una compra y no la paga sino que firma un recibo o resguardo, está haciendo uso del crédito. El emisor, luego, pagará las compras al comerciante adherido. Al efectuar esos pagos, el emisor está ejecutando el contrato de apertura de crédito combinado con el contrato de emisión de la tarjeta. Cuando el emisor paga al comerciante adherido, lo está haciendo con el dinero que puso a disposición del cliente.

El contrato de apertura de crédito es un contrato atípico, es decir no existe una regulación detallada en el derecho español sobre el mismo. Sólo se encuentra mencionado en el Código de Comercio (apartado 7 del art. 175 C. de c.)[335]. Sin embargo, ante esta falta de un marco jurídico especial, el

[335] A diferencia de la normativa española, en el Derecho comparado el art. 1.842. C.C. Italiano define la figura del contrato de apertura de crédito como aquel «contrato bancario por el cual la banca se obliga a tener a disposición de la otra parte una suma de dinero por un cierto periodo de tiempo o a tempo indeterminado»; Véanse JIMENEZ SÁNCHEZ, Guillermo J. (coord.). *Lecciones de derecho mercantil,* 10 ª ed. Madrid: Tecnos, 2005, p. 465; JAVIER CORTES, Luis. "Los contratos bancarios", en MENÉNDEZ, Aurelio. *Lecciones de derecho mercantil,* 3 ª ed. Navarra: Aranzadi, S.A., 2005, p. 656; CASTILLEJO MANZANARES, Raquel. *El juicio ejecutivo basado en pólizas bancarias*. Valencia: Tirant Lo Blanch, 1996, p. 71; MARIÑO LÓPEZ, A. *Responsabilidad civil*…op., cit., p. 41.

concepto de contrato de apertura de crédito ha sido desarrollado por la doctrina[336] y la jurisprudencia.

A juicio de algunos autores, el contrato de apertura de crédito es «aquel contrato por el cual el banco se obliga, dentro del límite pactado, y mediante una comisión que percibe del cliente, a poner a disposición de éste, y a medida de sus requerimientos, sumas de dinero o a realizar otras prestaciones que le permita obtener al cliente. Su elemento esencial es la disponibilidad o puesta a disposición del acreditado, de sumas de dinero a consecuencia de la concesión de un crédito, o mejor dicho, a consecuencia de la promesa de concederlo; por eso se habla de "apertura de crédito"»[337].

El contrato de apertura de crédito es definido como «aquel por el cual el acreditante, a cambio de la prestación de una comisión, se compromete, dentro los límites de cantidad y tiempo pactados, a conceder crédito al cliente (llamado acreditado), bien haciéndole entregas de efectivo o efectuando prestaciones que permitan obtener efectivo, o que generen un deber aplazado de pago que habrá de devolver en las condiciones pactadas»[338].

Alguna jurisprudencia española trata de definir este tipo de contrato. La STS de 27 de mayo de 1966[339] lo define como «un contrato por el que el Banco pone el dinero a disposición del cliente por cuantía y tiempo determinados»; y, en esta misma línea, la SAP de Zaragoza de 28 de abril

[336] Véanse JIMENEZ SÁNCHEZ, G. J. (coord.). *Derecho mercantil*…op., cit., p. 457; LINARES ANDRADE, Lucia. "La ejecución y preferencia de las pólizas bancarias de préstamo y apertura de crédito", en CUÑAT EDO, Vicente; y BALLARIN HERNANDEZ, Rafael. *Estudios sobre jurisprudencia bancaria*. Navarra: Aranzadi S.A., 2000, p. 251; BELTRAN SÁNCHEZ, Emilio M y ORDUÑA MORENO, Javier Fco (coords.). *Curso de Derecho Privado,* 7 ª. ed. Valencia: Tirant Lo Blanch, 2004, p. 696.

[337] GARRIGUES, Joaquín. *Contratos bancarios.* 2 ª. ed. Madrid: 1975, p. 185; ALCOVER GRAU, G*. Introducción al Derecho Mercantil*. Madrid: Editorial Dilex, S.L., 2008, p. 179.

[338] SÁNCHEZ CALERO, F. *Instituciones de Derecho Mercantil.* Madrid: MacGraw-Hill, 2002, p.337; también en. *Instituciones de derecho mercantil. Títulos-valores, contratos mercantiles, Derecho concursal y marítimo,* t II. 22 ed. Madrid: McGraw Hill, 1999, p. 318.

[339] *RA* 2746.

de 1982 califica al contrato de apertura de crédito como «aquel negocio jurídico bilateral por el cual el comerciante o entidad mercantil se obliga a tener a disposición de la otra parte una determinada suma de dinero, ya en numerario en efectivo, ya en efectos mercantiles o pago de deudas, por tiempo limitado o ilimitado, en cuyo caso es revocable a voluntad de la entidad concedente del crédito, y haciéndose constar en la cuenta corriente del beneficiario la cantidad por la que se concede el crédito y la cantidad o cantidades de que dispone la persona a quien el crédito se concede»[340].

Existen concepciones que lo equiparan a un contrato de préstamo[341]; sin embargo, dicha tesis es rechazada por la doctrina mayoritaria que se inclina

[340] AMESTI MENDIZABAL, C.: «El concepto de contrato de apertura de crédito y su diferenciación respecto al contrato de préstamo», en SÁNCHEZ CALERO, F.; CALERO GUILARTE, J. (coords.). *Comentarios a Jurisprudencia de Derecho Bancario Y Cambiario, v II. Consideraciones en entorno algunos aspectos de la cuenta corriente bancaria.* Madrid: 1993, p. 70, nº. 4; BROSETA PONT, M. y MARTÍNEZ SANZ, F. *Manual…op., cit.,* p. 243.

[341] GARRIGUES,J.: *Contratos…op..,* cit.p. 89, sostiene que "la perfección del contrato de apertura de crédito, a diferencia del préstamo, no depende de ninguna entrega de dinero, ya que incluso la entrega de dinero puede faltar cuando la ayuda prestada por la entidad de crédito a su cliente consista en prestarle su firma, interponiendo su garantía en las deudas e cliente"; en el mismo sentido SÁNCHEZ CALERO, F. señala que "el contrato de apertura de crédito se caracteriza por la disponibilidad, a favor del acreditado, pero ello no equivale a la disponibilidad propia de los depósitos del efectivo, sino que debe ser entendida como la facultad otorgada al cliente de tener acceso libre al patrimonio de la entidad acredítate, para que -dentro de los límites pactados- dicha entidad efectúa operaciones crediticias". Citado por DÍAZ MENDEZ, Nicolás. "Problemática procesal de la ejecución del contrato de apertura de crédito", en NIETO CAROL, U (coord.). *Contratos bancarios & parabancarios.* Valladolid: Lex Nova, 1898, p. 575; por su parte la SAP de Pamplona, de 18 de abril de 1989 diferencia el contrato de apertura de crédito y el contrato de préstamo «… el Banco prestamista entrega al cliente- prestatario una cantidad, objeto del préstamo en dinero, que puede entregárselo en cuenta corriente o similar, para que pueda disponer de el en el momento, por lo que se le transmite la propiedad de esa suma, y el banco es acreedor a su devolución desde dicho instante; mientras que en los de crédito o afianzamiento, por el Banco no se otorga ni se entrega al cliente ninguna propiedad ni disponibilidad del numerario en el momento, sino que se otorga un crédito o descubierto para operaciones mercantiles hasta un cierto límite…»; como pone de relieve BROSETA PONT y MARTÍNEZ SANZ, el contrato de apertura de crédito "se diferencia del contrato de préstamo bancario de dinero no solo en su carácter consensual (frente al carácter real que, en principio tiene el préstamo), sino, sobre todo, en el objeto de uno y otro contrato. El contrato de apertura de crédito consistiría en la propia disponibilidad de crédito (con independencia de que se haga uso o no de de él), tanto que en el préstamo el objeto contractual consistiría en la cantidad efectivamente entregado al prestatario", BROSETA PONT, M. y MARTÍNEZ SANZ, F. *Manual de…op., cit.,* p. 244. vid. CACHÓN BLANCO, José Henrique. "El contrato bancario de apertura de

a caracterizarlo como un contrato "sui generis" con sustanciales diferencias en relación al contrato de préstamo. Tesis que consideramos aceptable, ya que el contrato de apertura de crédito es un contrato consensual y bilateral con obligaciones para ambas partes, mientras que el de préstamo es un contrato real y unilateral, con una entrega única o varias fraccionadas[342].

El contrato de apertura de crédito tiene como elemento esencial el de garantizar al cliente la "disponibilidad de crédito", del que podrá hacer uso durante el tiempo convenido[343].

Cabe resaltar que el contrato de apertura de crédito también puede ser formalizado por vía electrónica o telemática[344].

3.2.1.1. *Caracteres*

Como ya se ha anticipado en otro epígrafe, el contrato de apertura de crédito se caracteriza por ser un contrato consensual y bilateral, no formal, a pesar de que suele estipularse por escrito[345], genera obligaciones para ambas partes[346] y es oneroso e *intuitu personae*, por cuanto el banco

crédito", en NIETO CAROL, U (coord.). *Contratos bancarios & parabancarios.* Valladolid: Lex Nova, 1998, pp. 541 y ss.

[342] VICENT CHULIÁ, Fco. *Introducción al*….op., cit*.,* p. 940.

[343] JAVIER CORTÉS, Luis. *Lecciones de contratos y mercados financieros*. Madrid: Civitas, 2004, p. 124; BELTRÁN SÁNCHEZ, E. M y ORDUÑA MORENO, J. Fco (coords.). *Curso de…*op*., cit.,* p. 696*;* PONT, M. y MARTÍNEZ SANZ, Fernando. *Manual de…op., cit.,* p. 244.

[344] MARTÍNEZ-SIMANCAS, Julián. "Contratos bancarios e Internet", en MATEU DE ROS, Rafael y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital.* Prólogo de Anna Birulés I Bertrán. Elcano (Navarra): Aranzadi, S.A., 2000, p. 491; vid. la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores,(*BOE*, núm. 166, 12 julio de 2007).

[345] Vid. BROSETA PONT, M. y MARTÍNEZ SANZ, F. *Manual de…op., cit.,* p. 244*.*

[346] Véanse las STSS de 27 de de mayo de 1966; de 21 de enero de 1985(RA 1990); SAP de Pamplona de 18 de 1989, ambas sobre la relación entre el banco y el cliente; VICENT CHULIÁ, Fco. *Introducción al…op., cit*., p. 940.

consiente la apertura de crédito en consideración a la solvencia moral y económica del acreditado[347].

Una de las obligaciones que tiene la entidad es conceder crédito a favor del cliente, es decir, poner a disposición del cliente las cantidades o realizar las prestaciones que éste le exija dentro de l os límites cuantitativos y temporales pactados[348].

En el contrato de apertura de crédito se dispone del mismo mediante el uso de número de la tarjeta, a través de comercio electrónico en el establecimiento adherido al sistema, para adquirir bienes y servicios, o para retirar dinero en l os cajeros automáticos o en o ficinas bancarias[349]. Por su parte, el cliente contrae las siguientes obligaciones[350]:

a) abonar a la enditad de crédito una comisión de apertura pactada[351]

b) reintegrar a la entidad de crédito la cantidad que haya dispuesto

c) satisfacer los intereses devengados por las sumas retiradas

[347] BETRÁN SÁNCHEZ, E. M y ORDUÑA MORENO, J. Fco (coords.). *Curso de…op., cit.,* 696 p; JIMÉNEZ SÁNCHEZ, Guillermo J. (coord.). *Lecciones de…*op., cit., p. 465.

[348] Véanse, BELTRÁN SÁNCHEZ, Emilio M y ORDUÑA MORENO, J. Fco (coords). *Curso de…op., cit.,* p. 696; JIMÉNEZ SÁNCHEZ, G. J. (coord.). *Lecciones de…*op., cit., p. 466; VICENT CHULIÁ, Fco. *Introducción al…op., cit*., p. 940; JAVIER CORTÉS, Luis. Los contratos bancarios…op., cit., p. 658; BARDAJÍ MUÑOZ, Luis. *Derecho mercantil. (Inspección de finanzas),* 4. ª ed*.* Madrid: Centro de Estudios Financieros, 1998, p. 26; CASTILLEJO MANZANARES, Raquel. *El juicio ejecutivo…op., cit.,* p.73*;* BROSETA PONT, M. y M ARTÍNEZ SANZ, Fernando. *Manual de…op., cit.,* pp. 244 y ss; GÓMEZ MENDONZA, M.: "tarjetas bancarias y cajeros automáticos", en NIETO CAROL, U (coord.). *Contratos bancarios & parabancarios.* Valladolid: Lex Nova, 1998, p. 862.

[349] GÓMEZ MENDONZA, M.: "tarjetas…"*op., cit*., p 862.

[350] Véanse BELTRÁN SÁNCHEZ, E. M y ORDUÑA MORENO, J. Fco (coords.). *Curso de…op., cit.,* p. 696; JIMÉNEZ SÁNCHEZ, G. J. (coord.). *Lecciones de…*op., cit., p. 466; JAVIER CORTES, L. "Los contratos bancarios…"*op., cit*., p. 658; BARDAJÍ MUÑOZ, L. *Derecho mercantil…op., cit.,* p. 26; BROSETA PONT, M. y MARTÍNEZ SANZ, F. *Manual de…op., cit.,* p. 245.

[351] Vid. CAHÓN BLANCO, J. H. "El contrato bancario*…"op., cit*., p. 560.

3.2.2. Contrato de mandato

Algunos sectores de la doctrina española relacionan el contrato de emisión de tarjeta con el contrato de mandato, señalando que la obligación principal que asume el emisor es la de abonar las órdenes de pago emitidas por el titular en el momento de celebrar el contrato de cambio con el establecimiento comercial adherido al sistema[352]. Cuando el titular presenta la tarjeta, suscribe en este instante una nota o cupón que constituye una orden de pago, a cargo del emisor, a favor del establecimiento comercial adherido al sistema.[353] También se considera como un mandato de pago o delegación de pago, en el que el mandatario está obligado a realizar el pago de obligaciones dinerarias por cuenta de su mandante[354].

3.2.3. Contrato de cuenta corriente bancaria

Como en el caso del contrato de apertura de crédito, el contrato de cuenta corriente bancaria carece de una regulación jurídica en el derecho español. No obstante, esta figura contractual aparece mencionada en los art. 175. 9º, 177 y 180 del Código de Comercio, así como en el Reglamento General del Banco de España de 1 948, (en los preceptos 46 y 98)[355]. Situación que ha llevado a la doctrina y a la jurisprudencia española a la necesidad de estudiar dicha figura contractual para conocer que similitud o diferencia plantea con otras figuras contractuales que carecen de una regulación en el derecho español.

---

[352] DIEZ-PICAZO, L y GULLÓN BALLESTEROS, A., *Sistema de derecho civil,* t II. Madrid: Tecnos, 1995, pp. 445 y ss.

[353] NUÑEZ LOZANO, P. *Tarjeta de*…op., cit., pp. 181 y ss.

[354] VICÉNTE CHULÍA, Fco. *Compendio critico de*…*op. cit*., p. 814.

[355] En el Derecho comparado, la legislación Argentina regula el contrato de cuenta corriente bancaria, en el art.771 del Código de Comercio, conceptualizándolo, «como aquel contrato bilateral y conmutativo, por el cual una de las partes remite a la otra, o recibe de ella en propiedad, cantidades de dinero u otros valores sin aplicación a empleo determinado, ni obligación de tener a la orden una cantidad o un valor equivalente, pero a cargo de acreditar al remitente por sus remesas, liquidarlas en las épocas convenidas, compensarlas de una sola vez hasta la concurrencia del débito y crédito y pagar el saldo».

3.2.3.1. *Concepto*

Como hemos indicado con anterioridad, la doctrina española se ha ocupado extensamente de esta figura contractual. Así, la define «como un contrato de gestión, en virtud del cual el Banco se compromete a realizar por cuenta de su cliente cuantas operaciones son inherentes al servicio de caja, realizando las correspondientes anotaciones contables»[356]. Hay quien la define como «un contrato neutro o de gestión, por el cual el banco se obliga a prestar al cliente el servicio de caja (ingresos y reintegros) y de contabilidad de todas las operaciones realizadas por dicha cuenta»[357].

Para algunos, es aquel contrato en el que «el cliente contrata con la entidad de crédito un "servicio de caja" que implica un mandato general de realización de cobros y mandatos específicos de pago, para los que el cliente realiza la correspondiente provisión de fondos. Incluye además un pacto de compensación automática de los cobros y los pagos de contabilización de los mismos por parte de la entidad de crédito»[358].

Sin embargo, hay sectores de la doctrina que defienden la concepción unitaria[359] del contrato de cuenta corriente, en el sentido de definirlo como «negocio jurídico en virtud del cual dos personas acuerdan anotar y compensar en cuenta abierta por Debe y Haber sus eventuales créditos recíprocos y, en su caso, establecen las condiciones de exigibilidad y disponibilidad del saldo o saldos resultantes de la compensación progresivamente operada»[360].

---

[356] GARIGUES. *Contratos…op., cit.,* 1979; EMBID IRUJO, José M.: "La cuenta corriente bancaria", en NIETO CAROL, Ubaldo (dir). *Contratos bancarios y parabancarios*. Valladolid: Editorial Lex Nova, S.A., 1998, pp. 36 y ss.

[357] VICENT CHULIÁ, F. *Introducción al…op., cit.,* p. 937.

[358] ALCOVER GRAU G. *Introducción al Derecho…* op., cit., pp. 175 y ss.

[359] MOLL DE MIGUEL, S. El *contrato de…o., cit.,* p. 209; DE EIZAGUIRRE, J. Mª. *Cuenta corriente bancaria y clausula "sin gasto" en la STS de 7 de marzo de 1974*. San Sebastián: 1978.

[360] MOLL DE MIGUEL, S. El *contrato de…op., cit.,* p. 209.

La SAP de Sevilla (sala 1ª) de 13 de diciembre de 1988, define el contrato de cuenta corriente como «un contrato especial, caracterizado por la existencia de un impacto que sobre la base de una mutua concepción de crédito, mantiene unidos los elementos integrantes de la cuenta, teniendo que hacerse efectiva su participación».

En el derecho comparado, la doctrina argentina ha destacado el concepto formulado por la Sala B de la Cámara Nacional de Apelaciones en lo Comercial, de 14 de septiembre de 1987, según la cual la cuenta corriente bancaria no es más que «un contrato de coordinación, no formal y de duración, nominado y autónomo, que se sustenta económicamente en los contratos de depósito en cuenta corriente y en la apertura de crédito, produciéndose como consecuencia del servicio de caja que brinda al cliente la obligación de cumplimentar las órdenes de sus clientes y poner a su disposición los fondos»[361].

Desde el punto de vista de las definiciones que hemos abordado a lo largo de este epígrafe, cabe señalar que lo característico de la cuenta corriente bancaria es el denominado "servicio de caja" como elemento esencial de la actividad de la entidad de crédito en la relación jurídica.

Una de las principales obligaciones de la entidad bancaria es cumplir las instrucciones del titular de la cuenta atendiendo las órdenes de pago que éste dé, a cambio de una comisión[362]. Otra de las obligaciones de la entidad bancaria es informar periódicamente al cliente sobre el estado de su cuenta mediante envío de extractos.

[361] ALEJANDRA MUCHART, María. *Contrato de cuenta corriente bancaria.* [En línea] disponible en Internet: http://www.buenastareas.com/ensayos/Contrato-De-Cuenta-Corriente-Bancaria/3055027.html (última consulta, 25 de noviembre de 2012).

[362] vid STS 21 de noviembre de 1997(R.8.096); SÁNCHEZ CALERO, F. *Instituciones de…op., cit.,* p. 325.

Como señala la doctrina[363], el deber de informar no puede limitarse únicamente al envío de extractos de cuenta en fechas determinadas, sino que se debe extender a la obligatoria comunicación de los saldos y envío de extractos cuantas veces y en los momentos que el cliente desee: SSTS de 11 de marzo de 1992, RJ.2.170, y de 15 de julio de 1993, RJ. 5805. El cliente debe manifestar su disconformidad con las partidas de los extractos en el plazo pactado: SSTS de 14 de junio de 1985, RJ. 3.270, y de 20 de junio de 2003.

Por su parte, el cliente tiene la obligación de pagar las distintas comisiones correspondientes a los servicios prestados, así como aportar fondos suficientes para que el banco pueda proceder a la realización de los pagos que procedan a favor de terceros[364].

3.2.3.2. *Las diferencias existentes entre el contrato de cuenta corriente bancaria y el contrato de cuenta corriente mercantil*

En la doctrina española existen dos corrientes doctrinal opuestas, una que es defendida por quienes son partidarios de diferenciar[365] las dos figuras contractuales y otra que defiende una concepción unitaria[366]. La primera corriente señala que "se debe rechazar la identidad entre cuenta corriente bancaria y cuenta corriente mercantil, simplemente por los siguientes motivos"[367]:

---

[363] SÁNCHEZ CALERO, F. *Instituciones de…op., cit*., p. 326; JAVIER CORTÉS, L. "Los contratos…"*op., cit.,* pp. 675-676.

[364] vid. Art. 250 C. c.; algunas Jurisprudencias considera esta operación de concesión de crédito (SSTS de 2 de octubre de 1984, 11 de julio de 1994).

[365] GARRIGUES, J. *Contratos…*op., cit., p. 120; a favor de esta vertiente SÁNCHEZ CALERO, F. «Contrato de cuenta corriente mercantil y el de cuenta corriente bancaria y rendición de cuenta», *RDBB,* 1992, pp. 545-546.

[366] En este sentido, MOLL DE MIGUEL, S. El *contrato de…op., cit.,* p. 209.

[367] GARRIGUES, J.: *Contratos…op., cit.,* p. 120; vid. JIMÉNEZ SÁNCHEZ, G.J. (coord.). *Lecciones de…*op., cit., 465 p; SÁNCHEZ CALERO, F. *Instituciones de…op., cit.,* p. 325; VICENT CHULIÁ, F. *Introducción*…op., cit., p. 937.

1. En la cuenta corriente bancaria no existe la reciprocidad de concesión de crédito, como sucede en la cuenta corriente mercantil[368]

2. Según la doctrina opuesta a la "vertiente unitaria", la indisponibilidad de los créditos comprendidos en la cuenta corriente mercantil desaparece en la cuenta corriente bancaria, ya que el cliente puede disponer en cualquier instante de su crédito con el fin de retirar el importe de su saldo[369]

3. En la cuenta corriente mercantil, la compensación entre la masa de los créditos y la de las deudas sólo se produce en el momento de cierre de la cuenta para dar lugar a un saldo exigible

4. Mientras que en la cuenta corriente bancaria los créditos entre el banco y cliente no sufren modificaciones: son inmediatamente exigibles, por lo que su anotación produce una compensación inmediata, impropia o puramente contable, reduciendo el saldo a favor del cliente, en una compensación automática[370]

Alguna jurisprudencia distingue las dos figuras contractuales mediante sentencias, como por ejemplo la de la Audiencia Provincial de Cáceres, de 8 de febrero de 1 988, que plantea que estas son figuras distintas; y la de Audiencia Provincial de Á vila, de 1 3 de diciembre de 1990 en el mismo sentido.

[368] Véanse GARIGUES. *Contratos*…op., cit., p. 120; VICÉNT CHULÍA, F. *Introducción al*…op., cit., p. 937; NÚÑEZ-LAGOS, Francisco. *Contratos bancarios*. Madrid: Centro de Formación del Banco de España, 1995, p. 119. éste autor señala que en la cuenta corriente "no existe la dación de crédito reciproco, sino unilateralidad del cliente al Banco, con consecuencia del depósito; del Banco al cliente, si se trata de una petición del crédito".

[369] GARIGUES, J.: *Contratos*…op., cit., p. 120.

[370] Ibídem, *Contratos*…op., cit., pp. 117 a 120 p; VICENT CHULÍA, F. *Introducción al*…*op., cit*., p. 937; NÚÑEZ-LAGOS, Fco. *Contratos…op., cit.,* p. 119.

3.2.3.3. *Caracteres jurídicos del contrato*

Se trata de un contrato consensual y no real ya que la entrega de fondos por parte del cliente tiene más bien la significación de provisión de fondos[371]. No es formal a pesar de que se celebre por escrito[372]. Es un contrato bilateral.

3.3. Contrato de pasarela de pagos o Terminal de Punto de Venta Virtual

3.3.1. Concepto y naturaleza jurídica

El contrato de "aceptación"[373], "afiliación"[374], "adhesión[375], "admisión de tarjeta de crédito como medio de pago"[376], o "contrato de pasarela de pagos o Terminal de Punto de Venta Virtual"[377], es aquel contrato celebrado entre la entidad emisora y/o gestora de la tarjeta y el proveedor de bienes o servicios, mediante el cual éste se obliga a admitir las tarjetas, ya sean de crédito o de débito, como medios de pago "on line" u "off line"[378]. Es una relación contractual básica para la eficacia del sistema de pago mediante tarjeta[379].

---

[371] JAVIER CORTÉS, L. "Los contratos…"*op., cit.,* p. 674; SÁNCHEZ CALERO, F. *Instituciones de…op., cit.,* p. 325.

[372] BROSETA PONT, M. y MARTÍNEZ SANZ, F. *Manual de…op., cit.,* p. 236.

[373] BARUTEL MANAUT, C. *Las Tarjetas de*…op., cit., p. 549.

[374] La Recomendación 87/598CE norma IV.3 emplea la palabra "afiliación". Presenta otras características, sinalagmática o bilateral y de ejecución continúa; GÓMEZ PRÚA, J. "La tarjeta de…"*op., cit.,* p. 191; GARCÍA SANZAZ, Arturo. «La retrocesión en el contrato de comercio electrónico», en MADRID PARRA, A (dir.). *Derecho patrimonial*. Prólogo de Manuel Olivencia. Madrid: Marcial Pons, 20007, pp.292 y ss.

[375] BATUECAS CALETRÍO, A. *El pago por medios electrónicos*…op., cit., p. 77.

[376] GETE-ALONSO y CALERA, M. C. *Las tarjetas*…op., cit., p. 84.

[377] Vid. RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo…", *op., cit*., p. 338;

[378] GETE-ALONSO y CALERA, M.C. *El pago mediante…op., cit.,* p. 24; SÁNCHEZ GOMEZ, A. *El Sistema de…*op., cit., op., cit., p. 15.

[379] BARUTEL MANAUT, C. *las Tarjetas de…op., cit.,* p. 549.

Como pone de relieve la doctrina[380], cuando la tarjeta es emitida para su empleo en establecimientos distintos de l os propios emisores, necesariamente ha de existir, con carácter previo a s u utilización, una relación contractual entre la entidad emisora --o la entidad de franquicia-- y el establecimiento comercial. Sin embargo, no s e producirá esta relación jurídica contractual cuando la tarjeta sólo pueda ser utilizada por el titular para adquirir bienes o servicios en el establecimiento del propio emisor[381], o sea, cuando coincide la figura de emisor y aceptante; por ejemplo, las tarjetas comerciales de El Corte Inglés, Alcampo y Carrefour entre otras. Por lo tanto, no existe en este caso contrato de aceptación ya que es el propio emisor quien acepta la tarjeta en su establecimiento.

En este sentido, estamos de acuerdo con quienes vienen señalando que "no se debe confundir el contrato de aceptación, con el que puedan suscribir diferentes emisores para dar un mayor servicio operativo a s us tarjetas, ni con los contratos de adhesión a l a red que los emisores franquiciados suscriben para entrar en un s istema de tarjeta; en estos casos se trata de contratos de colaboración"[382].

El contrato de aceptación de tarjeta es definido por algunos autores como "aquel en v irtud del cual el adquirente (distribuidor del sistema) y el aceptante (establecimiento comercial) acuerda la admisión, por éste último (en su establecimiento o en su cadena de establecimientos), de determinadas tarjetas emitidas por aquél u otros emisores, pertenecientes al

[380] GÓMEZ PRÚA, J. "La tarjeta de…"*op., cit.,* p. 195; BARUTEL MANAUT, C. *las Tarjetas de…* op., cit., p. 550.

[381] GETE-ALONSO y CALERA, M.C. *El pago mediante la tarjeta de crédito*. Madrid: La Ley, 1990, p. 24; BARUTEL MANAUT, C. *Las Tarjetas de…op., cit.,* p. 549.

[382] BARUTEL MANAUT, C. *Las Tarjetas de…* op., cit., p. 550. éste autor señala que "cuando se dan casos en la que una tercera entidad suministradora del sistema de tarjeta presta servicios directo a los titulares, como por ej.: servicios de caja automática, éste actúa de prestador, o sea de aceptante de tarjeta y no como emisor; no obstante el contrato en virtud del cual interviene y que le obliga a dicha aceptación de la tarjeta no es un contrato de aceptación con el emisor, sino un convenio de colaboración o adhesión a la red de la tarjeta, o a la otra con la que existe interoperabilidad". Criterio al cual compartimos.

sistema o los sistemas de tarjeta a los que se hallan vinculado/s, con el fin de que el titular pueda realizar transacciones económicas con tarjeta, cuyo pago al aceptante asume el adquirente, siempre que éste cumpla los requisitos que se le exigen para cerciorarse de la legitimidad de la transacción y de la titularidad de la tarjeta"[383].

3.3.2. Caracteres

Al igual que el contrato de emisión, se trata de un contrato mercantil, ya que responde a un acto de empresa ejercido dentro de su actividad[384]. El contrato de aceptación es un contrato atípico[385] que contiene una estipulación[386] a favor de tercero, por la que el establecimiento se compromete a admitir la tarjeta como medio de pago de los bienes, con garantía de su pago por el emisor, que cobra o descuenta una comisión del importe de las mismas. Sin embargo, hay que recordar que, al igual que el contrato de emisión de tarjeta, el contrato de aceptación no ha sido regulado en el derecho positivo español. Se basa en el principio de la autonomía de la voluntad de los contratantes (art. 1255 CC).

Es un contrato-tipo[387] que responde al sistema de negociación en masa por el adquiriente. Es un contrato complejo, denominado por el emisor contrato de afiliación[388]. Es un contrato consensual, que quedará

[383] BARUTEL MANAUT, C. *Las Tarjetas de*…op., cit., p. 551.
[384] Ibídem.
[385] En este mismo sentido GETE-ALONSO y CALERA señala que se trata de un contrato atípica por que se fundamenta en el principio de la autonomía de la voluntad contractual (art. 1255 CC), en GETE-ALONSO y CALERA, M.C. *El pago mediante*…op., cit., p. 24; MARIÑO LOPEZ, Andrés. *La responsabilidad civil…*op., cit., p. 53; SÁNCHEZ GÓMEZ, A. *El Sistema de…*op., cit., op., cit., p. 163; vid. SAP de Baleares, de 17 de noviembre de 2003.
[386] A favor de esta afirmación DE MARCHI, G. *«Carte di credito e*…op., cit., p. 329 y ss; DE ARRILLAGA, J. *La tarjeta…op., cit.,* p. 790; GÓMEZ PRÚA, J. «La tarjeta de…» *op., cit*., pp. 191 y ss; NUÑEZ LOZANO, P. *La tarjeta de…op., cit.,* pp. 201-214; en contra de esta posición BARUTEL MANAUT, C. *Las Tarjetas de*…op., cit., p. 557- 559; GETE-ALONSO y CALERA, M. *Las tarjetas…op., cit.,* p.96.
[387] SÁNCHEZ GÓMEZ, A. *El sistema…op., cit*., p. 162;
[388] vid. la SAP de Baleares, de 17 de noviembre de 2003, la cataloga como de "contrato de afiliación al sistema de tarjetas"

perfeccionado cuando el emisor o banco adquirente comunique al establecimiento la aceptación de su oferta de afiliación.

También se trata de un contrato de adhesión[389], ya que el establecimiento aceptante se adhiere al sistema de tarjeta sin discutir ni las cláusulas generales del contrato ni el funcionamiento. Es un contrato oneroso e *intuitu personae*, porque el adquiriente valora específicamente al establecimiento aceptante antes de ofrecerle la posibilidad de contratar[390].

En este tipo de contrato, las entidades emisora y/o gestora de la tarjeta se comprometen a pagar a dichos establecimientos o a los sistemas de tarjetas de crédito en los que éstas se encuentren incorporados, el importe de las órdenes de pago válidamente emitidas o autorizadas de acuerdo a las condiciones acordadas por las partes, dentro del marco del Reglamento.

Sobre la redacción del contrato de tarjeta, la Recomendación 87/598 CE, establece en su norma III. 1. a), que «los contratos celebrados entre los emisores o sus representante y los prestadores o consumidores revestirán la forma escrita y deberán ser objeto de una petición previa. Definirán con precisión las condiciones generales y especificas del acuerdo».

Con la celebración de este contrato, tanto la parte aceptante como la entidad emisora o el banco adquirente deberán cumplir una serie de obligaciones que serán estudiadas a lo largo de este capítulo. Sin tener que entrar en los detalles de las obligaciones que incumben a las partes intervinientes, nos gustaría hacer alusiones algunas de las principales obligaciones que corresponden a cada uno de ellos.

[389] SÁNCHEZ GÓMEZ, A. *El sistema…op., cit*., p. 162; GARCÍA SOLÉ, F. «Aspecto sobre la incidencia de la tecnología en el mercado de tarjeta», en Instituto Católico de Administración y Dirección de Empresas (ICADE), núm. 43 enero-abril, 1998, pp, 80 y ss.
[390] BARUTEL MANAUT, C. *Las Tarjetas de…*op., cit., p. 552.

Así, el proveedor de bienes o servicios tiene como obligación principal aceptar la tarjeta de crédito cuando el titular la presente como medio de pago, ya sea "off line" o mediante una transacción "on line", como hemos señalado en el capítulo III, ya que en las transacciones on line no se utiliza la propia tarjeta para efectuar el pago sino su número que, en su caso, puede ir acompañado de clave o PIN. Y a su vez, la entidad emisora o el banco adquirente tiene la obligación de facilitar el material necesario para la tramitación de operaciones con tarjeta (pasarela de pago TPV virtual) y la de efectuar el pago de las cantidades dispuestas por éste derivadas de su utilización[391].

3.4. Contrato de acceso a Internet

Se puede definir el contrato de acceso a Internet, como aquel contrato en virtud del cual una de las partes, el proveedor de acceso a la red, facilita a la otra, el cliente, ya sea titular de la tarjeta o proveedor de bienes o servicios, la conexión a Internet a cambio de un precio[392].

En otro orden de cosas, se puede caracterizar como un contrato atípico que se regirá por lo convenido entre las partes contratantes. De hecho, en lo no negociado entre las partes, se aplicará como régimen supletorio, la regulación del contrato de servicios (arrendamiento)[393]. Como señalan algunos autores, estamos ante "un contrato de larga duración, cuyo objeto en la práctica suele combinar junto a prestaciones de servicios (acceso a Internet, protección de datos…) la realización de obras por parte del proveedor –en el contexto de la distinción tradicional entre arrendamiento de obras y de servicios--, que implica, a diferencia de lo que sucede en la prestación de servicios, una obligación de resultado y no sólo de actividad (lo

[391] SÁNCHEZ GÓMEZ, A. *El sistema…op., cit*., p.162.
[392] DE MIGUEL ASENSIO, P. A. *Derecho...op., cit.,* p. 62.
[393] Según se prevé en el art. 1.544 C.C español, "en el arrendamiento de obras o servicios, una de las partes se obliga a ejecutar una obra o aprestar a la otra un servicio por precio cierto."

que puede plantearse en relación con la transmisión de mensajes de correo electrónico…)"[394].

3.5. Las obligaciones y cargas de las partes implicadas en la emisión y utilización de la tarjeta de pago en el comercio electrónico

Como ya hemos indicado a lo largo de esta investigación, la tarjeta de crédito es uno de los medios de pago más utilizados en el comercio electrónico, y tanto la LSP, LRLOCM, LCDSFC y TRLGDCU, como las distintas Recomendaciones comunitarias se han pronunciado sobre el pago mediante tarjeta. Estas regulaciones se centran básicamente y directa o indirectamente en los deberes de información, y las obligaciones y responsabilidades de los sujetos intervinientes en el pago mediante tarjeta en el comercio electrónico. Por lo que se refiere el contrato de emisión, aceptación y al contrato de cambio, establecen un conjunto de obligaciones a cargo de los sujetos intervinientes (emisor, titular, proveedor de bienes o servicios y banco adquirente).

Con el objeto de atribuir responsabilidad civil en el caso de operaciones no autorizadas o fraudulentas a los sujetos que intervienen en los distintos contratos donde se hace uso de la tarjeta de crédito como medio de pago electrónico, es necesario examinar las distintas obligaciones y cargas que se derivan de esta relación contractual vinculadas al sistema de pago electrónico.

3.5.1. Obligaciones y cargas del emisor de la tarjeta

El cumplimiento por parte de la entidad emisora de la tarjeta de sus obligaciones ha de valorarse en el marco de las relaciones que sustentan la

[394] DE MIGUEL ASENSIO, P.A. *Derecho…op., cit.,* p. 62 y ss.

operativa, al menos triangular, de pago[395]. En este sentido, podemos destacar como obligaciones básicas del emisor las siguientes:

1. La entrega de la tarjeta

Para evitar el uso ilegítimo de la tarjeta, la entidad emisora debe entregar la misma previa petición de su titular[396]. Como ha puesto de relieve la doctrina, «la obligación del emisor no se agota con el simple hecho de entregar de la tarjeta; éste ha de prestar su asistencia constante para el disfrute del servicio contratado. Supone la obligación de sustitución de la tarjeta en los casos de caducidad, deterioro y pérdida o sustracción»[397].

En este sentido, la Recomendación 88/590/CE, en el punto 5 del anexo, señala dos aspectos: primero plantea que «el contrato entre el emisor y el titular se considerará celebrado una vez que éste haya recibido el instrumento de pago y un ejemplar de las cláusulas contractuales por él aceptadas». Se ha de resaltar que el contrato sólo debe considerarse celebrado una vez que el titular recibe la tarjeta y firma el contrato para marcar así el inicio de su vigencia.

También en este mismo punto 5 de la Recomendación 88/590/CE, se establece la prohibición del envío no solicitado de la tarjeta, es decir «no se enviará ningún instrumento de pago a un cliente, a menos que éste así lo haya solicitado expresamente». Igualmente, la Recomendación 97/489/CE, prevé en su art. 7.2 b) que «no se enviará un instrumento electrónico de pago sin una previa solicitud, excepto cuando se trate de la reposición de un

[395] Vid. RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgos…" *op., cit.,* p. 349.

[396] Véanse, LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., p. 247; *SAP*, Barcelona, de 29 junio de 2000(AC 2000/ 3768); GETE-ALONFO y CALERA, M.C.: *Tarjeta de*… op., cit., p. 53; SÁNCHEZ GÓMES, A. *Sistema…op., cit*…p. 18; GÓMEZ MENDOZA, M. "Tarjeta…"*op., cit.,* p. 389; MARIÑO LÓPEZ, A. *Uso fraudulento de...op., cit.,* p.29.

[397] BARUTEL MANAUT, C. *Tarjeta de*…op., cit., p. 329; GÓMEZ MENDOZA, M. "Tarjeta…"*op., cit.,* p. 389.

instrumento electrónico de pago que ya poseía del titular». En esta misma línea, el inciso b) del art. 28 de la LSP, prevé que el proveedor de servicios de pago, en este caso emisor de un instrumento de pago, debe «abstenerse de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago».

El párrafo segundo de este mismo inciso b) del art. 28 de la LSP, señala que "esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente".

2. *Obligación de entregar un documento en la que se encuentra plasmado el contrato*

La obligación de entregar una copia de las condiciones contractuales va ligada a la obligación de entrega de la tarjeta que desarrollamos al inicio. La Recomendación de la Comisión 88/590/CE es muy explícita en el punto 5, al afirmar que el contrato entre el emisor y el titular se "considerará celebrado una vez que éste haya recibido el instrumento de pago y un ejemplar de las cláusulas contractuales por él aceptadas".

Sobre el mismo punto, la Recomendación de la Comisión 97/489/CE plantea en su art.3.1 la información mínima que debe figurar en las condiciones aplicables a la emisión y utilización de un instrumento electrónico de pago. Al firmar el contrato o, en cualquier caso, con la suficiente antelación antes de la entrega de un instrumento electrónico de pago, el emisor comunicará al titular las condiciones relativas al contrato (en lo sucesivo denominadas las «condiciones») aplicables a la emisión y utilización del instrumento electrónico de pago. Las condiciones incluirán una indicación de la ley aplicable al contrato. Estas condiciones se harán constar

por escrito y, en su caso por medios electrónicos, términos claros, fácilmente comprensibles y, al menos en una lengua oficial del Estado miembro donde se ofrezca el instrumento electrónico de pago[398].

Resumiendo, cabe resaltar que en el comercio electrónico a través de Internet existe la obligación de entregar una copia de las cláusulas contractuales y ello se hará por medios electrónicos, correspondiendo a la entidad emisora las obligaciones de garantizar o habilitar los mecanismos técnicos que permitan tanto leer a través de la página web como recibirla por correo electrónico y descargar y mantener en el ordenador o mediante cualquier *soporte* o *instrumento* (el CD-ROM, DVD, tarjeta de memoria y el dispositivo USB[399]) que permite al titular conservar el texto de las cláusula contractuales y acceder ulteriormente a ellas. Esto en la Ley del contrato de seguro se denomina "*soporte duradero*"[400].

---

[398] Vid. PANIZA FULLANA, Antonia. *Contratación a distancia y defensa de los consumidores. Su regulación tras la reforma de la Ley de Ordenación de Comercio Minorista y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Granada: Comares, 2003, p. 313.

[399] Según se establece en el art. 5.3 de la LCCG, "cuando el contrato no deba formalizarse por escrito y el predisponente entregue un resguardo justificativo de la contraprestación recibida, bastará con que el predisponente anuncie las condiciones generales en un lugar visible dentro del lugar en el que se celebra el negocio, que las inserte en la documentación del contrato que acompaña su celebración; o que, de cualquier otra forma, garantice al adherente una posibilidad efectiva de conocer su existencia y contenido en el momento de la celebración"; por su parte, la Condición Decimoséptima(condiciones especiales para la contratación telemática) de Bankia, prevé en el punto 17.3. "(…): si la contratación del servicio se hubiera realizado mediante el servicio de oficina de Internet de Bankia o por cualquier medio a través de Internet: por escrito que será remitido al domicilio señalado por el titular de la presente Solicitud-Contrato o mediante la orden de impresión on–line realizada a través de Internet, o bien mediante cualquier soporte o instrumento que permita al titular conservar o imprimir la información y, en particular, las disquetes informáticos, CD-ROM, DVD, así como el disco duro del ordenador que permite la descarga de los archivos conteniendo la documentación contractual o donde se almacene el correo electrónico del Titular,…".

[400] Según se establece en la disposición adicional primera de la Ley 50/1980, de 8 de octubre, del Contrato de Seguro, se entiende por *soporte duradero* "siempre que esta Ley exija que el contrato de seguro o cualquier otra información relacionada con el mismo conste por escrito, este requisito se entenderá cumplido si el contrato o la información se contienen en papel u otro soporte duradero que permita guardar, recuperar fácilmente y reproducir sin cambios el contrato o la información", en *BOE*, núm. 250, de 17 de octubre de 1980; sobre este mismo aspecto ver el apartado 2 del art. 6 bis,

3. Obligación de guardar en secreto los datos del titular

Mediante la celebración del contrato de emisión de tarjeta, la entidad emisora de la misma está obligada a guardar en secreto los datos confidenciales del titular (número de identificación o código)[401], y de modo seguro, para que éstos no puedan ser interceptados por un tercero que después los utilice fraudulentamente[402]. En la misma línea, la Condición General del contrato de tarjeta de Caja Madrid[403], prevé en su punto 8.1 la obligación de Bankia de mantener secretos los NIP asignados al titular de la tarjeta.

Siguiendo lo expresado por la Audiencia Provincial de Tarragona (Sección 3ª) en su sentencia de 27 de diciembre de 2004, la entidad emisora tiene como obligación "la de mantener secreto el PIN y anular la tarjetas caducadas y denunciadas, entre otros extremos porque el PIN sea conocido por persona distinta a su titular. La diligencia en el cumplimiento de esas obligaciones no puede tener el mismo rasero, pues la del cliente consumidor conforme al artículo 1104 del Código Civil ha de ser la genérica de un padre de familia, atemperada siempre a las obligaciones impuestas y explicitadas en el contrato suscrito, mientras que la diligencia de la entidad bancaria es la exigible a un profesional, dado que es la entidad bancaria la que confecciona el sistema y dispone al caso de los cajeros, su diseño y medidas de seguridad, por ende en mayor disposición para corregir los fallos que se producen en dicha seguridad".

[401] Vid., la SAP de Navarra, de 20 de enero de 1999(AC 1999/3018); BOQUERA MATORONA, Josefina. "El impago de la deuda por la entidad emisora de la tarjeta de crédito", en CUÑAT EDO, Vicente y BALLARIN HERNANDEZ, R. (dirs). *Estudios sobre jurisprudencias bancarias.* Navarra: Aranzadi, S.A., 2000, p. 393; La Ley Orgánica 15/1999, de 13 de diciembre, sobre protección de datos de carácter personal, define en su artículo 3, a) *que los datos de carácter personal: «cualquier información concerniente a personas físicas identificadas o identificables».*

[402] GETE-ALONSO y CALERA, M. C. *Tarjeta de… op., cit*., p. 53.

[403] Vid. Condiciones Generales sobre la obligación de Bankia, punto 8.1

Sentado ello, corresponde a la entidad bancaria, conforme a las reglas de la carga probatoria fijadas en el artículo 217 de la Ley Enjuiciamiento Civil, acreditar que el cliente ha sido negligente o no ha tenido la diligencia exigible en la conservación de la tarjeta o en guardar secreto del PIN (así sentado en sentencias de Audiencia Provincial Toledo 1/7/1999, Málaga (sección sexta) 23/7/2002 y Madrid (sección 12ª) 6/10/2004), mientras que corresponde al usuario de la tarjeta acreditar que las disposiciones efectuadas con su tarjeta son fraudulentas, es decir, no realizadas por él ni tampoco con su autorización, distribución de la carga probatoria respetada por la Juez de Instancia".

Según establece el artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[404], bajo el título "deber de secreto", «el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo».

Por otra parte, la Recomendación de la Comisión 87/598/CE[405], en sus puntos 4 b) y c), prevé la protección de seguridad, y establece en el inciso b) que «al efectuar el pago, los datos transmitidos al banco del prestador y, posteriormente, al emisor no afectarán, en ningún caso, a la protección de la vida privada. Se limitarán estrictamente a los datos previstos normalmente para cheques y transferencias. Y en el punto c) determina que todos los problemas que plantean la protección de los datos y la seguridad deberán

[404] España: «Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado» en *BOE*, núm. 298, de 14 de diciembre de 1999, 12 p.

[405] Vid COMISIÓN EUROPEA (1987): Recomendación de la Comisión, de 8 de diciembre de 1987, «relativa a un código europeo de conducta referente a los pagos electrónicos», (87/598/CEE), *Diario Oficial* núm. L 365 de 24/12/1987, pp. 0072-0076.

ser claramente expuestos y resueltos, en todas las etapas, en los contratos entre las partes»[406].

La Recomendación de la Comisión 88/590/CE, establece en el punto 4.3 que «las cláusulas contractuales impondrán al emisor la obligación, frente al titular, de no revelar el número o código de identificación personal, o en su caso, otros datos de naturaleza igualmente confidencial sino al propio titular».

En este mismo sentido, la Recomendación de la Comisión 97/489/CE, prevé igualmente en su sección III, art. 7.2 a), que el emisor «no revelará a terceros el número de identificación personal del titular u otro código, excepto al propio titular».

Lo cierto es que si la obligación que corresponde al emisor de entregar la tarjeta no va unida a un número o código de acceso (NIP)[407] y dirigida a proporcionar la suficiente información al titular sobre el funcionamiento de la tarjeta, es decir, con informaciones necesarias sobre cómo conservar y a la vez hacer el uso correcto de la misma, dicha obligación sería insuficiente[408].

4. *Obligación de poner a disposición del titular de la tarjeta los medios de comunicación adecuados para que éste pueda notificar el robo, extravío o situaciones de riesgos de utilizaciones fraudulentas de la tarjeta*

La entidad emisora está obligada a poner a disposición del titular todos los medios necesarios a fin de que esta pueda cumplir con su deber de notificación "sin demora indebida" del extravío, sustracción u otras

[406] Vid. BARUTEL MANAUT, C. *Tarjeta de*…op., cit., pp. 373 y ss.
[407] Vid. SAP de Navarra, de 20 de enero de 1999(AC 1999/3018); GÓMEZ SÁNCHEZ, A.: *El sistema…*op., cit*.,* p. 20.
[408] BARUTEL MANAUT, C, *Tarjeta de…op., cit.*, pp. 351-352; vid. GÓMEZ SÁNCHEZ, A.: *El sistema…*op., cit*.,* p. 84; GÓMEZ MENDOZA, M.: *Tarjeta…op., cit.,* p. 392.

situaciones como por ejemplo, la suplantación de los datos bancarios en la red[409].

Con respecto a este punto la Ley 16/2009, de servicios de pago, hace hincapié en la obligación que incumbe el proveedor de servicios de pago (emisor de la tarjeta), de «garantizar que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar la comunicación indicada en el artículo 27.b, o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 26.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma» (art. 28. C). Resulta razonable dicha medida, ya que en el caso de que no se notifique esta circunstancia traerá consecuencias para el usuario.

Por su parte, la Recomendación de la Comisión 88/590/CE, en el punto 8.1, establece que todo emisor «facilitará los medios por los que sus clientes puedan notificar, a cualquier hora del día o de la noche, la pérdida, robo o falsificación de sus instrumentos de pago; pero en el caso de las tarjetas comerciales, sólo podrá disponerse de dichos medios de notificación durante las horas de apertura de las empresas emisoras».

Por otra parte, la Recomendación de la Comisión 97/489/CE dispone en su art.7.2 d) que «garantizará la existencia de medios adecuados para permitir al titular efectuar la notificación prevista en la letra b) del artículo 5. En caso de que dicha notificación se hiciere por teléfono, el emisor (o la

[409] En este mismo sentido RODRÍGUEZ DE LAS HERAS BALLELL, quien sostiene que la entidad emisora debe implantar mecanismos necesarios para facilitar al titular el cumplimiento de su carga de comunicar la pérdida o sustracción de la tarjeta y adoptar las medidas oportunas para la cancelación de la tarjeta con mayor brevedad, RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo…", *op., cit.,* p. 353.

entidad por él indicada) proporcionará al titular los medios que acrediten que dicha notificación ha sido efectuada por el titular».

Sobre lo planteado en el párrafo anterior, también debe ser citada la sección IV, art. 9.1 de la Recomendación de la Comisión 97/489/CE, en la que se establece que «el emisor (o la entidad especificada por él) proporcionará los medios para que el titular, en cualquier momento del día o de la noche, pueda notificar la pérdida o el robo de su instrumento electrónico de pago».

Creemos que con el objetivo de minimizar los riesgos que puedan surgir a consecuencia de la sustracción o extravío de la tarjeta, la entidad emisora debe contar con un sistema de recepción, ya sea por la vía telefónica o por medios electrónicos; en este último caso, enviando un correo electrónico a la oficina central que opere las veinticuatro horas del día, identificando y registrando cada una de las denuncias realizada por los titulares.

Por último, hemos de resaltar que es necesario que dichas notificaciones por vía telefónica sean gratuitas; es decir, que las entidades emisoras deben al menos facilitar una línea de atención al cliente que atienda solamente casos relacionadas con las emergencias, sobre todo la sustracción, extravío y suplantación de la identidad, a la que se puedan efectuar llamadas desde cualquier teléfono, ya sea móvil o fijo, sólo marcando el número de emergencia, sin tener que costear dicha llamada.

5. Obligación de informar al titular periódicamente sobre las operaciones por él realizadas mediante el envío de un extracto

Es la obligación de la entidad emisora de facilitar al titular la información sobre su estado de cuenta (resumen de las operaciones realizadas con la

tarjeta)[410] a través de la página web de la entidad o por otros medios. Con el objetivo de que el titular compruebe las regularidades de los mismos o el estado de su cuenta[411]. Sobre esta misma línea, la Condición General del contrato de tarjeta de Bankia[412] establece, en su punto 9.3, la obligación de Caja Madrid de " facilitar periódicamente al titular un extracto de las transacciones realizadas con la tarjeta que permitan su identificación".

La Recomendación de la Comisión 88/590/CE, establece en su punto 6.3, que «se facilitará al titular, cuando así lo solicite, un extracto de sus operaciones, inmediatamente o poco después de su realización; no obstante, cuando se trate de un pago en el punto de venta, el recibo de caja facilitado por el detallista en el momento de la compra, y que contendrá las referencias al instrumento de pago, deberá reunir los requisitos de la presente disposición».

La norma comunitaria no establece expresamente la obligación de entregar al titular de la tarjeta una relación de las operaciones realizadas durante un periodo de tiempo, lo que precisa es que el extracto se extenderá a petición del titular inmediatamente o poco después de la operación[413]. Esta obligación se puede dividir en dos:

a) la entrega de un comprobante resumen de las circunstancias de cada operación realizada, de acuerdo al contrato de emisión

[410] MARIÑO LÓPEZ, A. *Uso fraudulento de tarjeta…*op., cit., p.105; BOQUERA MATARREDONA, J. "El impago de…"*op., cit.,* p. 393; vid. RODRÍGUEZ DE LAS HERAS BALLELL T. "El reparto de riesgo…", *op., cit.,* p. 350.

[411] LAFUENTE SÁNCHEZ, Raúl. *Los servicios financieros*…op., cit., 248 p; MARIÑO LOPEZ, L. *Responsabilidad contractual*…op., cit., p.125; GETE ALONSO Y CALERA, M. *Tarjeta de…op., cit.,* p. 59; BARUTEL, *Tarjeta de*…op., cit., pp. 364 y ss.

[412] Vid. Condiciones Generales sobre la obligación de Caja Madrid, punto 8.1

[413] BARUTEL, *Tarjeta de*…op., cit., pp. 365 y ss; MARIÑO LÓPEZ, L. *Uso fraudulento de tarjeta…*op., cit., p. 105.

b) la entrega de una relación de la operatoria efectuada durante un determinado periodo, con expresión de los datos principales de la misma, para su seguimiento y comprobación por el titular

La Recomendación de la Comisión 97/489/CE establece en su art.3.3 e) que «las condiciones de contrato de emisión deben contener el período de tiempo durante el cual el titular puede impugnar una transacción dada y una indicación de las vías de recurso y procedimientos de reclamación a su disposición y del método para acceder a ellos. Lo que presupone el envío de de la información de los pagos realizados con el instrumento de pago electrónico con el motivo de hacer posible el control del titular»[414].

6. Obligación de garantizar todos los medios de seguridad

Se trata de aquella obligación que tiene el emisor frente al proveedor de bienes o servicios de entregarle el material necesario con el fin de asegurar el buen funcionamiento del sistema e impedir el uso indebido o fraudulento del mismo, ya sea por el titular o por un tercero no autorizado. Se trata de la obligación que permite garantizar la seguridad a la hora de efectuar operaciones de pago electrónico; esta obligación será cumplida una vez que el emisor pone a disposición del prestador de bienes o servicios los terminales de punto de venta (TPV), bases de datos, aplicación informática de la web de banca electrónica y pasarela de pago[415].

Se trata de un deber de colaboración del emisor de mantener los medios técnicos y los dispositivos a través de los que opera la tarjeta en el estado adecuado para permitir que pueda utilizarse la misma[416].

[414] ibídem
[415] BAUTECAS CALETRIO, A. *Pago con*... op., cit., p. 270 y ss; BOQUERA MATORONA, J. "El impago de…"*op., cit*., p. 393; LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., p. 248.
[416] GETE ALONSO Y CALERA, M.C. *Tarjeta de…*op., cit p. 59; GÓMEZ SÁNCHEZ, A. *El sistema…*op., cit., pp.105 y ss.

Desde el punto de vista del comercio electrónico es interesante la reflexión de algunos autores, tras afirmar que la "obligación de prestar soporte técnico ha de reconducirse, ya no a la instalación de los dispositivos físicos (TPV) y su mantenimiento, sino a la instalación del software de procesamiento de pagos (pasarela de pagos) –residente en el servidor seguro de la emisora- cuya incorporación al procedimiento de contratación del proveedor de bienes y servicios se articula mediante una licencia de uso sobre la aplicación informática"[417].

Además de las obligaciones examinadas con anterioridad, también le corresponde al emisor la obligación de atender los pagos o disposiciones en efectivo efectuados por el titular de la tarjeta en los sitios web o tiendas virtuales adheridos al sistema[418], y en su caso, a través de medios electrónicos.

3.5.1.1. *Cargas del emisor*

En este epígrafe se analizará de forma muy breve, lo que alguna doctrina considera no tanto obligaciones del emisor cuanto cargas del mismo. Para ello es preciso, en primer lugar, definir en qué consiste la carga; y en segundo lugar, analizar los supuestos de cargas negociales en el contrato tarjetas de crédito.

Concepto de la carga

Según precisa algún autor[419], "para perfilar el concepto de la carga en el, ámbito del Derecho sustantivo, es preciso tener en cuenta el significado

[417] RODRÍGUEZ DE LA HERAS BALLELL, T. "El reparto de riesgo…", *op.*, *cit.,* p. 340.

[418] BAUTECAS CALETRIO, A. *El pago por medios electrónicos: una aproximación a las tarjetas.* obra Social y cultural de caja de Segovia: 2000, p. 82; GETE ALONSO Y CALERA, M.C. *Tarjeta de…*op., cit p.50; NUÑEZ LOZANO, P. L. *La tarjeta…*op., cit. p. 177; vid., art. 4.3 y anexo 2 i) Directiva 87/102 de Crédito al consumo; art. 6.3 de la Recomendación de la comisión 88/590/CE; art. 7 de la Recomendación de la comisión 97/*489/CE.*

[419] CABANILLAS SÁNCHEZ, Antonio. *Las cargas del acreedor en el derecho civil y en el mercantil.* Madrid: Editorial Montecorvo, S.A., 1998, pp. 43 y ss, Según sostiene este autor,

de la carga en el Derecho procesal". Ya que, "las cargas procesales implican la necesidad de realizar determinados actos para evitar que sobrevengan perjuicios procesales". Añade que, "se trata de «imperativos del propio interés», no existiendo una obligación de llevar a cabo el acto procesal en que consiste la carga".

Este mismo autor[420], sostiene que "semejante a lo que acontece en el Derecho procesal, en el Derecho sustantivo la esencia de la carga no radica tanto en la idea de coactividad". Es decir, "la carga opera como premisa del buen resultado de la propia acción o interés. Por ello, tanto en el Derecho procesal como en el Derecho sustantivo se afirma que la carga es un «imperativos del propio interés» para evitar un perjuicio; lo que indica la libertad del sujeto de ejercer o no la conducta en que consiste la carga, o sea no está obligado a cumplirla, aunque su observancia es necesaria para realización del interés".

Resumiendo, cabe señalar que la carga es una conducta del acreedor que ha de observar en su propio interés para que pueda ejercitar una facultad[421]. Queda demostrado que la carga no es objeto de una obligación, sino que implica la necesidad de observarla para la realización del propio interés.

Para continuar con el estudio de este epígrafe, nos parece fundamental resaltar que existen dos modalidades de carga del acreedor, el

---

que el camino acertado para precisar el concepto de la carga ha sido perfectamente señalado por la doctrina alemana, tras poner de relieve que la carga no constituye un *sollen*, sino un *müssen*, es decir un «tener» que para «poder hacer». Y a continuación señala que, desde esta perspectiva la carga es una conducta del acreedor que ha de observar en su propio interés para que pueda ejercitar una facultad",

[420] *Ibídem*, op., cit., p. 44.

[421] *Ibídem*, op., cit., p. 44.

heterónomo[422] y las negociales. No obstante, estudiaremos estas últimas (las cargas negociales en el contrato de tarjeta de crédito que son afines a nuestra investigación), que son todas aquellas que emanan directamente del contrato suscrito entre las partes, que es frecuente que figuren en contratos de adhesión[423].

a) Mantener un registro interno que garantice la prueba de las transacciones efectuadas con tarjeta.

Mantener o llevar registros internos que garanticen la prueba de las operaciones efectuadas con tarjeta, como señala la doctrina, se tiende a configurar como una obligación en algunas de las Recomendaciones que analizaremos a continuación.

La Recomendación 88/590/CE establece en el punto 6.1 de su Anexo: «en lo que respecta a las operaciones a que se hace referencia en el punto 1(pago por medios electrónicos que suponga el uso de tarjeta, especialmente en el punto de venta), los emisores llevarán o procurarán que se lleven registros internos suficientemente detallados, de manera que quede constancia de dichas operaciones y puedan rectificarse los errores. A este fin, los emisores se concertarán con los suministradores de sistemas sobre las medidas necesarias»[424].

Por su parte, el punto 6.2 de esta misma Recomendación establece que «en cualquier controversia con el titular en relación con cualquiera de las operaciones a que se hace referencia en el primer, segundo y cuarto guión del punto 1 y en lo que respecta a la responsabilidad por una transferencia

[422] *Ibídem,* op., cit., p. 62. las cargas heterónomas son aquellas cargas que derivan de la Ley y la buena fe negocial.
[423] *Ibídem*, op., cit., p. 62
[424] Véanse, SÁNCHEZ-CALERO GUILARTE, Juan. «La Armonización comunitaria de los sistema de pago electrónicos (tarjeta)», *Noticias CEE*, Madrid, 1989, año 5, núm. 58; BARUTEL MANAUT, C. *Tarjeta de*…op., cit., p. 359.

de fondos por medios electrónicos no autorizada, corresponderá al emisor probar que la operación fue correctamente registrada y correctamente contabilizada, y que no resultó afectada por alguna avería técnica o cualquier otra anomalía».

La Recomendación de la Comisión 97/489/CE, establece en el art. 7.2 c), que «el emisor mantendrá un registro interno durante un período de tiempo suficiente para que quede constancia de las transacciones a que se refiere el apartado 1 del artículo 1 y se puedan rectificar los posibles errores»; y por último, el inciso e), de la referida Recomendación dispone que «en caso de litigio con el titular en relación con una de las transacciones especificadas en el apartado 1 del artículo 1, y sin perjuicio de cualquier prueba en contrario que el titular pueda producir, demostrará que la transacción ha sido registrada y contabilizada correctamente, y que no se ha visto afectada por un fallo técnico o por cualquier otra anomalía».

A pesar de lo planteado en las dos Recomendaciones que se citan, consideramos bastante acertada la doctrina que se inclina a conceptualizar este registro como una carga[425]. Existen, del mismo modo, opiniones de los tribunales que se han pronunciado sobre este tipo de cargas[426].

b) Impedir la utilización de la tarjeta una vez recibida la notificación de robo, o extravío, entre otras, por su titular

Corresponde a la entidad emisora impedir la utilización del medio de pago una vez que se le ha notificado su extravío, robo, caducidad o uso incorrecto, de fondos disponibles[427]. En esta misma línea, la Recomendación de la Comisión 88/590/CE establece en el punto 8.4 que «el emisor, una vez

[425] Véanse, GETE ALONSO Y CALERA, M.C. *Tarjeta de…*op., cit., 60 p*;* BARUTEL MANAUT, C. *Tarjeta de*…op., cit., pp. 355 y ss; GÓMEZ SÁNCHEZ, A. *El sistema…op., cit.,* pp.122 y ss.

[426] Véanse la SAP de Alicante de 18 de enero de 1993(AC 1993/35); SAP Alicante de 30 de enero de 1995 (AC 1995/ 129); SAP de Barcelona de 2003 (JUR 2003, 107727).

[427] BATUECAS CALETRIO, A. *Pago con...*op., cit., p.276.

recibida la notificación, deberá, incluso en el supuesto de que el titular haya obrado con grave negligencia o fraudulentamente, procurar por todos los medios a su alcance impedir la ulterior utilización del instrumento de pago».[428]

El apartado 2 art.9 de la Recomendación de la Comisión 97/489/CE, establece que «una vez recibida la notificación, el emisor (o la entidad especificada por él), incluso en el supuesto de que el titular haya actuado con negligencia grave o de forma fraudulenta, deberá procurar, por todos los medios razonables a su alcance, impedir la ulterior utilización del instrumento electrónico de pago».

En este mismo sentido, según pone de manifiesto el legislador español en la nueva Ley de servicios de pago, el proveedor de servicios de pago tiene la obligación de "impedir cualquier utilización del instrumento de pago una vez efectuada la notificación a que se refiere el artículo 27. b)" (art. 28. d LSP)[429]. Es decir, cuando el usuario o el titular de la tarjeta notifican al emisor el extravío, sustracción o la utilización indebida, este último deberá impedir cualquier utilización de la tarjeta.

Por su parte, la Condición General del contrato de tarjeta de Bankia[430] prevé, en el punto 9.4, la obligación de la Caja Madrid como emisor de la tarjeta de «proceder a anular inmediatamente las tarjetas, comunicándolo a todas las entidades incorporadas a la red de servicios ofrecidos por ella en cualquiera de las siguientes circunstancias:

(i) cuando se notifica el extravío, hurto, robo de una tarjeta o el conocimiento de su PIN por terceras personas contra la voluntad del titular

[428] GÓMEZ MENDONZA, M. "Tarjeta…"*op., cit.,* p. 393.
[429] Ley 16/2009 de...*op., cit.*, p. 21.
[430] Vid. Condiciones Generales sobre contrato de tarjeta de Bankia

(ii) cuando tenga conocimiento de la no recepción de una nueva tarjeta

(iii) una vez llegada la fecha de caducidad de una tarjeta».

3.5.2. Obligaciones y carga del titular

Para atribuir al titular de la tarjeta de crédito la responsabilidad civil por el uso fraudulento de ésta, es imprescindible examinar las diversas obligaciones y cargas que le corresponden, a los efectos de determinar si dicha situación ilícita se ha dado por el incumplimiento de éstas[431].

En virtud del contrato de emisión de la tarjeta celebrado con la entidad emisora, al titular de la misma le corresponden varias obligaciones, cuya finalidad es prevenir el uso fraudulento de los datos de la tarjeta de crédito o débito en las operativas de pago a través de Internet, por personas ajenas o un tercero no autorizado.

1. Obligación de utilizar correctamente la tarjeta de pago

De acuerdo al contrato suscrito con la entidad emisora[432], se le impone al titular de la tarjeta la obligación de firmar la tarjeta[433], hacer uso correcto y

[431] MARIÑO LÓPEZ, L. *Uso fraudulento de tarjeta…* op., cit., p. 111.

[432] Estamos en presencia de un contrato de adhesión, nominativo, intransferible, sinalagmático, de ejecución continuada y temporal; vid. la SAP de Madrid de 23 de julio de 1995; SAP de Barcelona de 17 de enero de 1992; La condición general de Caja Inmaculada establece seis puntos sobre las obligaciones que debe asumir el titular de la tarjeta:
*"*a) En cuanto a la posesión de la Tarjeta:

1.- Firmar la Tarjeta a su recepción en el espacio destinado a tal fin.

2.-Conservar la Tarjeta que se le entrega en concepto de depósito y cuya propiedad corresponde a la Caja y tomar todas las medidas razonables para proteger la Tarjeta y los medios, tales como la clave secreta o PIN, que le permiten utilizarla.

3.-No anotar en la Tarjeta la clave secreta ni en ningún otro objeto que el titular habitualmente guarde o lleve con la Tarjeta. Así como no usar como clave secreta números que coincidan con fechas que el titular lleve en otros documentos junto a la Tarjeta (fechas de nacimiento etc.).

4.- Notificar a la Caja inmediatamente la pérdida, hurto, robo, uso indebido o falsificación de la Tarjeta o de los medios que permiten utilizarla, especialmente el conocimiento por parte de terceras personas de la clave secreta, personándose en su oficina y entregando en los casos que corresponda copia de la denuncia hecha ante autoridad nacional o extranjera competente. Esta notificación podrá anticiparse a través de llamada telefónica al Centro de Tarjetas habilitado a estos efectos o mediante comparecencia personal en cualquier oficina de la Caja.

adecuado de la misma, así como de garantizar la seguridad en su uso[434]. Es decir, el titular de la tarjeta está obligado a hacer uso de la misma en el sitio web o tienda virtual adherida al sistema[435], no hacer uso de este medio de pago electrónico una vez expirado su plazo de validez[436]. O sea, que el titular no podrá emplear la tarjeta como medio de pago o instrumento de pago una vez que está vencido el plazo establecido en el contrato de emisión.

Al mismo tiempo deberá custodiar y conservar de forma adecuada la tarjeta[437] y a su vez mantener en secreto la clave de acceso o el número de identificación personal (NIP) que se le asigna[438]; es decir, el titular debe custodiar y guardar diligentemente la tarjeta y los datos relacionados con la

---

5.- Devolver a la Caja la Tarjeta o Tarjetas concedidas en los supuestos de invalidación o cancelación de las mismas, resolución del contrato para su utilización o cancelación de la cuenta asociada a la Tarjeta, contempladas en la cláusula 3. Esta obligación de devolución existirá también en caso de bloqueo de la cuenta en virtud de mandato judicial, disposición legal o mediando justa causa que la Caja acreditará a su titular, así como en el caso de fallecimiento de alguno de sus titulares, por parte de los herederos del fallecido.

6.- Destruir la Tarjeta caducada".

[433] BARUTEL, C *Tarjeta de*…op., cit., pp. 419-420.

[434] LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., p. 251; RODRÍGUEZ DE LAS HERAS BALLELL, T. *El reparto de riesgo*…op., cit., p. 336; GÓMEZ SÁNCHEZ, A. *El sistema…op., cit.,* pp. 125 y ss; según BATUECAS CALETRIO, "con la inclusión de esta obligación lo que se pretende es evitar que el titular hace uso de la tarjeta cuando no dispone de fondos suficientes en su cuenta corriente a la que está adscrita", BAUTECAS CALETRIO, A. *Pago con tarjeta de…op., cit*., 244 p; BOQUERA MATORONA, J. "El impago de…"*op., cit*., p. 391; GÓMEZ MENDOZA, M. "Tarjeta…"*op., cit.,* p. 886.

[435] Como se venía reiterando con anterioridad que la utilización de la tarjeta como medio de pago en una red abierta como internet, es virtual, ya que la tarjeta no se exhibe ante el proveedor de bienes o servicios; Según GÓMEZ MENDOZA, la doctrina viene apuntando que en lo referente a la utilización de la tarjeta "no hay, por supuesto obligación de usar la tarjeta sino, caso de optar por ello, de hacerlo según las instrucciones indicados en el contrato", GÓMEZ MENDOZA, M. "Tarjeta…"*op., cit*., p. 401.

[436] LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., 251; GETE ALONSO y CALERA, M. C. *Tarjeta de…op., cit*., p. 64*;* BARUTEL, C. *Tarjeta de*…op., cit., pp. 428-439.

[437] La Recomendación 97/489/CE, expresa en su art. 5*.* c), «que el titular, no anotará su número de identificación personal u otro código de forma fácilmente reconocible, especialmente en el instrumento electrónico de pago o en cualquier objeto que guarde o que lleve junto con el mismo».

[438] GETE ALONSO Y CALERA, M. C. *Tarjeta de…op., cit.,* pp. 64-65*;* BARUTEL, *Tarjeta de*…op., cit., pp. 421-428; GÓMEZ SÁNCHEZ, A. *El sistema…op., cit.,* pp.128 y ss; RIVERO ALEMÁN, S. *Crédito, Consumo y…op., cit.,* p. 538.

misma, tomando las medidas razonables de seguridad personalizadas y todas las precauciones necesarias a fin de evitar el uso fraudulento de los datos de la tarjeta (número, fecha de caducidad, código de seguridad (CVV2 o CVV) y nombre del titular, entre otras), y adoptar las medidas necesarias que le permitan tomar conocimiento inmediato de dicha circunstancias.

En este sentido, la ya citada Sentencia de la Audiencia Provincial de Tarragona (Sección 3ª), de 27 de diciembre de 2004, en el epígrafe que corresponde a las obligaciones del emisor de la tarjeta, se establece en uno de sus fundamentos de derecho, que "el titular de la tarjeta (…) ostenta como obligaciones la conservación correcta y con precaución de la tarjeta y mantener en secreto el PIN; no anotar el PIN en la tarjeta ni en documento que se lleve o transporte junto dicha tarjeta y notificar de forma inmediata la pérdida, robo o falsificación de la tarjeta y el conocimiento por otras personas contra su voluntad del número de Identificación personal".

Por su parte, la condición general del contrato de tarjeta de Bankia[439] prevé en el punto 7.1 "la obligación del titular de la tarjeta de conservar la misma una vez que se le entrega en concepto de depósito cuya propiedad corresponde a Bankia, y utilizarla exclusivamente de conformidad con las instrucciones contenidas en la solicitud-contrato y las que, en su caso, se faciliten en cada momento".

La Recomendación 97/489/CE, establece en su art. 5.a), la obligación del titular de que éste «utilizará el instrumento electrónico de pago en las condiciones aplicables a la emisión y utilización de tales instrumentos; en particular, tomará todas las medidas adecuadas para garantizar la seguridad del instrumento electrónico de pago y de los medios. (NIP u otro código) que permitan su utilización».

[439] Vid. Condiciones Generales sobre la obligación de Bankia, punto 8.1.

Según dispone la nueva Ley de Servicios de Pago, "el usuario del instrumento de pago deberá utilizar el instrumento de pago de conformidad con las condiciones que regulen su emisión y utilización, en particular, en cuanto reciba el instrumento de pago, el usuario deberá tomar todas las medidas razonables a fin de proteger los elementos de seguridad personalizados de que vaya provisto" (art.27 inciso a))[440].

También, la Recomendación 88/590/CE establece en el punto 4.1.a), que las cláusulas contractuales impondrán al titular la obligación, frente al emisor, de «tomar las debidas precauciones para garantizar la seguridad del instrumento de pago y del procedimiento (por ejemplo, el número o código de identificación personal) que le permiten utilizarlo».

El inciso c) de la misma Recomendación señala que las cláusulas contractuales impondrán al titular la obligación «no anotar en el instrumento de pago el número o código de identificación personal del titular ni tampoco en cualquier otro documento que el interesado conserve o transporte con el instrumento de pago, especialmente si existe la posibilidad de que se pierda, se robe o se falsifique al mismo tiempo que aquél»[441].

Siguiendo el criterio sostenido por la doctrina[442], no se trata de que el titular esté obligado, efectivamente, a utilizarla, sino cuando ejercite el contenido contractual, o sea, cuando pretenda adquirir bienes o servicios con ella, o extraer dinero en los cajeros habilitados al efecto, de acuerdo a las instrucciones que se estipularon en el contrato de emisión[443].

[440] Ley 16/2009, de...*op., cit*., p. 19; en este mismo sentido, la Directiva 2007/ 64/CE, establece en su art. 56 a) la obligación del titular de la tarjeta.
[441] BARUTEL MANUT, C. *Tarjeta de*…op., cit., p. 425.
[442] GETE ALONSO Y CALERA, M. C. *Tarjeta de…op., cit.,* p. 64.
[443] SAP de Baleares, de 17 de julio de 2002(AC 2002, 2036), citado por SÁNCHEZ GÓMEZ, A. *El sistema…op., cit.,* pp. 126 y ss, nota al pie. 202

En la actualidad existen diversas sentencias españolas que hacen alusión al cumplimiento de la obligación de conservar y custodiar la tarjeta de pago. Entre ellas cabe señalar[444] la SAP de Bilbao, de 19 de diciembre de 1986, sobre el robo de una tarjeta del interior de un vehículo ; la parte demandante sostiene negligencia grave por parte del titular en su custodia; sin embargo, la Audiencia Provincial pone de manifiesto que «…corresponde al titular de la tarjeta un deber de custodia que, desde luego, puede generar responsabilidad, pese a que, al propio tiempo, no incluya la adopción de medidas de diligencia excepcional sino simplemente (art.1104 C.C) la que corresponde a las circunstancias de las personas, del tiempo y del lugar, exigiéndose, en definitiva la diligencia que correspondería a un buen padre de familia(…) No puede considerarse que dejar la tarjeta en el interior del vehículo suponga falta de diligencia en la custodia de la tarjeta, pues es

[444] Vid. Condiciones Generales sobre la obligación de Bankia punto 8.1

[444] Véanse, la SAP de Baleares, de 20 de marzo de 2003 (JUR 2003, 199769); según señala, la SAP de Tarragona, de 27 de diciembre, en su Fundamento de Derecho Tercero*, "que solo se le puede exigir al cliente una mínima diligencia, por ser la parte más débil en un contrato de adhesión",* citado por SÁNCHEZ GÓMEZ, A. *Sistema…op., cit.,* 23 p, *nota al pie 94;* la SAP Barcelona (sección 17ª), de 25 de enero de 1999 (AC1999/3165); La SAP Madrid núm. 48/ 2003(sección 8ª), de 8 de noviembre de 2004 (JUR 2004/89327); la SAP Castellón (Sección 1ª) de 30 de diciembre de 2004(AC2005/24), resuelve un caso relacionado con la desaparición de la tarjeta, sin que el titular comunicase a la entidad emisora de su desaparición, según la tesis de la Audiencia el titular actúa con falta de diligencia en la conservación de su tarjeta de crédito cuando ilocalizado durante 18 días, tiempo transcurrido durante el cual se efectúan operaciones fraudulentas con ella. Comentada por MERIÑO LÓPEZ, A. *Uso fraudulento*…op., cit., pp. 116-117; la SAP de Asturias (Sección 5ª), de julio de 2002 (JUR 2002/252307) se trata de un robo con fuerza, en la cual se forzaron la cerradura de la puerta de un camión dentro del cual se encontraba la tarjeta de crédito, y el titular toma conocimiento de su sustracción y uso indebido cuando recibe el extracto bancario. Según la AP, «El titular actuó de forma negligente al haber dejado de tomar de forma inmediata las medidas de comprobación pertinentes acerca de las consecuencias del robo una vez que comprobó que la cerradura de una de las puertas del camión había sido forzada, actuando tan solo cuando el banco le envía los cargos». También, se pone de manifiesto que existe una responsabilidad compartida con la entidad emisora, ya que esta incumple la obligación de verificación de la regularidad de las operaciones efectuadas con la tarjeta de crédito*;* criterio similar adoptada por la SAP de Girona (Sección 1ª) 9 de junio de 2005(JUR 2005/181562). SAP de Madrid de 8 de abril de 1999(AC1999, 1160); SAP de Toledo de 1 julio de 1999 (AC 1999, 1739*);* SAP de Palencia de 3 de febrero de 1999 (AC 1999, 442); SAP de Baleares de 25 de junio de 1999(AC 1999, 8828)

obvio que no puede adquirir el compromiso de llevarla siempre encima, amén de que, como es obvio, tampoco así se excluye el riesgo de robo».

En cambio, existen opiniones de los tribunales que ponen de relieve que dejar la tarjeta en un vehículo es un supuesto de negligencia grave[445]. Al respecto se pronuncia la SSAP Castellón (sección 2ª) de 12 de febrero de 2000[446] y (sección 1ª) de 26 de octubre de 1998[447].

Por último, reafirmando lo antes dicho en este punto, le corresponde al titular de la tarjeta tomar las medidas adecuadas para garantizar la seguridad de los datos de la tarjeta de pago utilizada en Internet y de los medios que permitan su utilización, por ejemplo, el ordenador. Dichas medidas pueden ser actualizar el antivirus, contar con un cortafuego (firewall) o no mantener abierta su sesión.

2. No anular una orden que haya dado mediante su instrumento de pago

Sobre esta obligación el punto 4.3 a) de la Recomendación de la Comisión de 1987 y el punto 4.1 d) de la Recomendación de la Comisión 88/590/CE, establece que las cláusulas contractuales impondrán al titular la obligación de «no anular una orden que el titular haya dado mediante su instrumento de pago». De la misma forma, la Recomendación de la Comisión 97/489/CE establece en su art. 5 d) que el titular «no revocará una orden que hubiere cursado mediante su instrumento electrónico de pago,

[445] En contrata de estas tesis, BATUECAS CALETRIO, pone de manifiesto que "un hecho importante que se debería tener en cuenta cuando se valora la negligencia del titular en estos casos es si están juntos el NIP y la tarjeta, porque este hecho si resulta esencial para que tenga éxito la utilización fraudulenta de la tarjeta. De esta forma, el titular no será negligente cuando le roban el NIP de su vehículo, si la tarjeta no está al alcance, porque dejar objetos o utensilios en el coche, observando las debidas medidas de precaución como ocultarlas o no dejarlas visibles (…) entra dentro de la diligencia media exigible. Sin embargo, que si debería responder cuando deja juntos la tarjeta y el NIP o cuando los deja fácilmente alcanzables o visibles". Tesis al cual consideramos correcto, en BATUECAS CALETRIO, A.: *Pago con tarjeta…op., cit.,* p. 269.

[446] (*AC* 2000, 753).

[447] (*AC* 1998, 2131).

salvo en caso de que el importe no se hubiere determinado en el momento de cursar la orden».

Como señala la doctrina, la irrevocabilidad de las operaciones es esencial a la tarjeta, especialmente para dar seguridad al sistema y a todos los que intervienen en él, principalmente a los aceptantes que en su actuación dentro del sistema de tarjeta deben tener seguridad del pago[448]

Además, corresponde al titular de la tarjeta cumplir con las siguientes obligaciones: obligación de pagar la cuota de emisión y mantenimiento; y obligación de pagar las deudas derivadas de la utilización de la tarjeta, en caso de mora.

3.5.2.1. *Carga del titular*

a) Comunicar el extravío, sustracción o el uso fraudulento de la tarjeta

El uso indebido o fraudulento de la tarjeta en la contratación a distancia se puede producir como consecuencia del extravío o sustracción de la tarjeta por un tercero no autorizado o cuando éste se apodera de los datos de la tarjeta y de la identidad del titular con el fin de utilizarlos en las operativas de pago a través de Internet. A raíz de estos supuestos[449], es de resaltar que, en el caso que el titular de la tarjeta tenga conocimiento del uso fraudulento o suplantación de la identidad, debe notificarlo al emisor "sin

[448] Vid. BARUTEL, C. *Tarjeta de*…, op., cit., pp. 435 y ss; SÁNCHEZ GÓMEZ, A. *El sistema…*op., cit. pp.131 y ss.

[449] LAFUENTE SÁNCHEZ, Raúl. *Los servicios financieros…op., cit*., p. 251; GETE ALONSO Y CALERA, M. *Tarjeta de…op., cit.,* p. 65; BARUTEL, *Tarjeta de*…op., cit., pp. 468-484; NUÑEZ LOZANO, Pablo Luís. *La tarjeta…*op., cit., pp. 367 y ss; CARBNEL PINTANEL, J.C. *La protección del consumidor…*, op., cit., 303 p, véanse SAP de Valencia de 26 de abril de 1993, sobre falta de aviso inmediato de la sustracción; SAP de Madrid de 11 de abril de 1987; y SAP de Sevilla de 31 de enero de 1995, citados por BOQUERA MATARREDONA, J. "El impago de…", *op., cit*., p. 391; vid. RUIZ MUÑOZ, Miguel. «El uso fraudulento de tarjetas de pago en la Directiva 2007/65/CE: La obligación de notificación y reclamación del usuario», en BOSH CAPDEVILA, Esteve (dir.). *Derecho de contractual Europeo. Problemática, propuestas y perspectivas.* Barcelona: Bosch, 2009, p. 127; vid; CABANILLAS SÁNCHEZ, A. *Las cargas del…*op., cit., 321 y ss.

demora indebida". Al respecto, el inciso c) del art. 27 de la LSP dispone que: «en caso de extravío, sustracción o utilización no autorizada del instrumento de pago, notificarlo sin demoras indebidas al proveedor de servicios de pago o a la entidad que éste designe, en cuanto tenga conocimiento de ello».[450]

Por otro lado, la Recomendación de la Comisión 88/590/CE, de 17 de noviembre de 1988, establece en el punto 4.1, b) que el titular tiene la obligación de notificar al emisor o a la agencia central, sin excesiva demora:

i) la pérdida, robo o falsificación del instrumento de pago o de los medios que hacen posible su uso

(ii) el cargo en la cuenta del titular de cualquier transacción no autorizada

(iii) cualquier error o irregularidad en la gestión de la cuenta por parte del emisor

Igualmente, la Recomendación de la Comisión 97/489/CE, establece en su art. 5. b) que el titular notificará sin demora al emisor (o a la entidad especificada por éste) en cuanto tenga conocimiento de ello: «la pérdida o el robo del instrumento electrónico de pago o de los medios que permitan su utilización, el registro en su cuenta de cualquier transacción no autorizada y cualquier error u otra anomalía en la gestión de su cuenta por parte del emisor».

Por su parte, la Condición General del contrato de tarjeta de Bankia[451] prevé en su punto 7.6 la obligación del titular de "notificar de inmediato a Bankia el robo, hurto o extravió de las tarjetas que podrá hacerse telefónicamente a la oficina de Bankia de la que sea cliente el titular o

[450] Sobre este mismo aspecto, véanse el apartado primero, inciso b) de la Directiva 2007/64/CE(DOUE, L319/36, de 5 de diciembre de 2007).
[451] Vid. Condiciones Generales del contrato de tarjeta de Bankia

beneficiario, mediante comparecencia personal en dicha oficina o en cualquier otra de Caja Madrid, o bien efectuando llamada telefónica al centro de tarjetas habilitado a este fin, o a través de Oficina Internet y Oficina Telefónica".

Asimismo, podrá efectuarse la notificación a través de cualquier entidad financiera concertada con Bankia que acepte la tarjeta como instrumento de crédito, ya sea en España o en el extranjero. A su vez, el titular o beneficiario deberá completar su notificación mediante la entrega o remisión a Bankia, a la mayor brevedad posible, de una copia de la denuncia hecha ante la autoridad nacional o extranjera competente, indicando fecha y hora en que ocurrieron los hechos. En el caso de que el titular o el beneficiario recuperen con posterioridad las tarjetas deberá entregarlas a Bankia para su anulación.

Sobre la carga de notificar o comunicar la pérdida o sustracción de la tarjeta de crédito, no existen opiniones unánime por parte de la jurisprudencia española; algunas sentencias "consideran que el retraso de 38 días en comunicar a la entidad emisora la sustracción de la tarjeta no se considera suficiente para generar responsabilidad en el titular de la misma (SAP, de Baleares de 26 de febrero de 1997)[452]", otras sostienen que "es diligente la comunicación efectuada el primer día hábil siguiente a aquel en que se verificó la sustracción"(SAP de Bilbao de 19 de diciembre de 1986[453]) y algunas aprecian la negligencia una vez que han transcurrido más de tres meses (SAP Málaga de septiembre de 19994).

Por su parte, la SAP de Baleares (Sección 5ª), de 25 de junio de 1999, resuelve el recurso de apelación interpuesto por el titular de la tarjeta sobre la sustracción o extravió de la misma que había sido juzgado por la Primera

[452] (AC 1997-3 21115) comentada por FARRADO MIGUEL, I y CASTAÑER CODINA, J. "Atribución y distribución de responsabilidad civil por uso no autorizado de tarjetas", *RDBB*, núm. 81, marzo 2001. Citado por LUNAS DIAS, María José (dir.). Malas prácticas bancarias

[453] (La Ley 1987-2),

Instancia. El juzgado declaró la responsabilidad del titular de la tarjeta porque consideró que había actuado culposamente al demorarse cinco días en comunicar la sustracción o extravió de la tarjeta de crédito[454].

b) Comunicar al emisor cualquier anomalía o irregularidad relacionada con la cuenta asociada a la tarjeta[455].

Cuando el titular recibe los extractos bancarios o resumen de las operaciones realizadas con su tarjeta, debe proceder a comprobar la regularidad de las mismas y, en caso de existir una anomalía o discrepancia que detecte en su cuenta, ya sea una operación no autorizada o un error de gestión, debe notificar al emisor de dichas irregularidades[456].

Sobre la carga del titular la Recomendación de la Comisión 88/590/CE, la califica como una obligación que corresponde al titular; en el punto 4.1b) se determina que «las cláusulas contractuales impondrán al titular la obligación, frente al emisor, de notificar al emisor o a la agencia central, sin excesiva demora, el cargo en la cuenta del titular de cualquier transacción no autorizada y cualquier error o irregularidad en la gestión de la cuenta por parte del emisor».

La Recomendación de la Comisión 97/489/CE, en su art. 5.b), incluye como obligación del titular, «la de notificar sin demora al emisor (o a la entidad especificada por éste), en cuanto tenga conocimiento de ello, el registro en su cuenta de cualquier transacción no autorizada y cualquier error u otra anomalía en la gestión de su cuenta por parte del emisor».

---

[454] En cambia la SAP (AC 1999, 8828), comentada por MARIÑO LÓPEZ, A. *Uso fraudulento…op., cit*., p. 124; SSAP de Valencia de 26 de abril de 1993 sobre falta de aviso inmediato de la sustracción y 20 de febrero de 1995 en la que esta Audiencia sostiene que, cumplida la obligación de comunicar la sustracción por el titular de la tarjeta, tiene la obligación de pagar.

[455] GETE ALONSO Y CALERA, M. C. *Tarjeta de…*op., cit., p. 65.

[456] CABANILLAS SÁNCHEZ, A. *Las cargas del…op., cit.,* pp. 321 y ss.

La Recomendación de la Comisión 87/598/CE establece en la Disposición Complementaria IV, punto 2, que «el consumidor titular de la tarjeta adoptará las precauciones razonables para garantizar la seguridad de la tarjeta emitida y observará las condiciones específicas (pérdida o robo) del contrato que haya firmado».

c) No anotar en el instrumento de pago o en cualquier otro documento o soporte electrónico el número o el PIN

La Condición General del contrato de tarjeta de Bankia prevé, en su punto 7.5, que el titular o beneficiario "no deberá anotar el PIN en la tarjeta ni en ningún otro objeto que habitualmente guarde o lleve con la tarjeta. Y que cualquier daño o perjuicio que pueda sobrevenirles por incumplimiento de esta obligación será de su exclusiva responsabilidad".

El punto 4.3 c), de la Recomendación de la Comisión 88/590/CE prevé que las cláusulas contractuales impondrán al titular la obligación de «no anotar en el instrumento de pago el número o código de identificación personal del titular ni tampoco en cualquier otro documento que el interesado conserve o transporte con el instrumento de pago, especialmente si existe la posibilidad de que se pierda, se robe o se falsifique al mismo tiempo que aquél».

Igualmente la Recomendación de la Comisión 97/489/CE establece en su art. 5. c) que el titular «no anotará su número de identificación personal u otro código de forma fácilmente reconocible, especialmente en el instrumento electrónico de pago o en cualquier objeto que guarde o que lleve junto con el mismo».

Teniendo en cuenta lo establecido en las distintas recomendaciones comentadas en este inciso, se ha de resaltar que en la operativa de pago mediante tarjeta en el comercio electrónico, corresponde al consumidor o

usuario titular de la tarjeta la obligación o el deber de no almacenar los datos bancarios y personales en su ordenador. Es decir, debe tomar todas las precauciones necesarias para conservar el código de acceso, el PIN y los demás elementos de seguridad.

Por otra parte, debe evitar abrir y/o contestar correos electrónicos de terceros, mensajes de texto, o comunicaciones sospechosas provenientes de remitentes que desconozca, o sea, evitar abrir mensajes provenientes de un spam o phising.

Además, el usuario no debe visitar sitios no seguros (por ejemplo aquellos que empiezan por "http") que pudieran insertar spyware o algún otro sistema para extraer información confidencial en su ordenador, así como bajar cualquier contenido de tales sitios y/o descargar sistemas o programas de cómputo que permitan compartir archivos (P2P) que pudieran vulnerar la privacidad de su información.

Cabe señalar, que el nivel de diligencia dependerá del tipo de usuario, ya sea: joven/mayor, profesional/ no profesional o informado /no informado.

Por último, hemos de concluir señalando que el cumplimiento de las obligaciones y cargas que corresponden al titular de la tarjeta son imprescindibles en el sentido de determinar la responsabilidad ante cargo fraudulento o indebido, puesto que el incumplimiento de dichas obligaciones puede traer consigo la exoneración, tanto por parte de la entidad emisora, como del proveedor de bienes o servicios, ambos intervinientes en la operativa de pago mediante el uso de la tarjeta de crédito o débito en Internet.

3.5.3. Obligaciones y cargas del proveedor de bienes o servicios

Los proveedores de bienes o servicios deben cumplir las mismas obligaciones que corresponden a los establecimientos comerciales

tradicionales o físicos en relación al tratamiento de los datos personales. En el caso de que se trate de un proveedor inscrito en el territorio español tendrá que cumplir con lo establecido en la Ley 15/1999, de Protección de Datos y en la Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información.

Las obligaciones que corresponden al establecimiento comercial adherido al sistema de pago electrónico frente a las partes intervinientes son[457]:

1. Obligación de aceptar la tarjeta

Como hemos señala con anterioridad, el contrato de aceptación, adhesión o de pasarela de pago al sistema de tarjeta, celebrado entre el emisor y el proveedor de bienes o servicios, tiene como finalidad imponer a éste último, como obligación principal, la de aceptar la tarjeta como medio de pago de las ventas realizadas o de los servicios prestados, siempre cuando aparezca como válida[458]. Una vez que el establecimiento acepta la tarjeta como medio de pago, éste deberá exigir al titular que firme la factura, (comprobando que dicha firma coincide con la estampada en la tarjeta) o la introducción del PIN.

Sin embargo, en la operativa de pago con tarjeta a través de Internet, no se puede exigir al cliente o el titular de la tarjeta que firme la factura, con el objetivo de comprobar si la firma coincide o no, ya que estamos ante un

[457] BOQUERA MATARREDONA, J. "El impago de…" *op., cit*., p.392. a juicio de éste autor, no se le puede imponer un pacto de exclusiva utilización de una determinada tarjeta de pago. El comerciante puede adherirse a cuantos sistemas de pago electrónico considera oportuno, nota p 25.

[458] Véanse, BATUECAS CALETRIO, A. *Pago con...op., cit*., pp. 280-281; SÁNCHEZ GÓMEZ, A. *El sistema…op., cit*., p. 171.

contrato a distancia en el que existe la ausencia física de una de las partes[459].

2. *Obligación de disponer de adecuados medios tecnológicos, materiales y publicitarios*

Como se ha señalado en el epígrafe anterior, la obligación principal del proveedor de bienes o servicios adherido al sistema, frente a los titulares de la tarjeta, es la de admitir o aceptar en su tienda virtual la tarjeta como instrumento de pago de las ventas realizadas o de los servicios prestados, siempre cuando aparezca como válida[460].

[459] Según se prevé en el Considerando(20) de la Directiva 2011/83/UE, «la definición de contrato a distancia debe abarcar todos los casos en que los contratos se celebran entre el comerciante y el consumidor en el marco de un sistema organizado de venta o prestación de servicios a distancia, exclusivamente mediante el uso de uno o varios medios de telecomunicación (venta por correo, Internet, teléfono o fax), hasta el momento en que se celebra el contrato, con inclusión de ese momento. Dicha definición debe cubrir también las situaciones en las que el consumidor únicamente visita el establecimiento mercantil de la empresa con el propósito de recabar información sobre los bienes o los servicios y la negociación y celebración subsiguiente del contrato tienen lugar a distancia. Por otra parte, un contrato que se negocie en el establecimiento mercantil del comerciante y acabe celebrándose a través de un medio de telecomunicación no debe considerarse un contrato a distancia. Tampoco debe considerarse un contrato a distancia el contrato que se inicie utilizando un medio de comunicación a distancia pero acabe celebrándose en el establecimiento mercantil del comerciante. Asimismo, el concepto de contrato a distancia no debe incluir las reservas que el consumidor pueda realizar a través de una técnica de comunicación a distancia para solicitar a un profesional la prestación de un servicio, como puede ser el caso de un consumidor que llame por teléfono para pedir una cita en una peluquería. El concepto de sistema organizado de prestación de servicios o de venta a distancia debe incluir los sistemas ofrecidos por un tercero distinto del comerciante pero utilizado por este, como una plataforma en línea. No obstante, no debe cubrir los casos en los que las páginas web ofrecen información solamente sobre el comerciante, sus bienes o servicios y sus datos de contacto», en Directiva 2011/83/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo", en *DOUE.* L 304/64, 22 noviembre de 2011; en este mismo sentido, el apartado 7 del art.2 de la Directiva 2011/83/UE, define el «contrato a distancia» como, "todo contrato celebrado entre un comerciante y un consumidor en el marco de un sistema organizado de venta o prestación de servicios a distancia, sin la presencia física simultánea del comerciante y del consumidor, y en el que se han utilizado exclusivamente una o más técnicas de comunicación a distancia hasta el momento en que se celebra el contrato y en la propia celebración del mismo".

[460] BARUTEL MANAUT, Carles, *Las tarjetas de pago y crédito*, op., cit., p. 603.

No obstante ésto, no podrá darse cumplimiento a dicha obligación sin observar previamente otras conductas. Como por ejemplo, la de contar con adecuados medios tecnológicos, materiales y publicitarios, así como la de utilizarlos adecuadamente y la de instruir a sus empleados sobre el funcionamiento de la tarjeta de crédito[461].

Como señalan algunos autores "éstas son las llamadas obligaciones integrativas instrumentales, como especificaciones y extensiones de la principal de aceptación de la entrega, de manera que su incumplimiento podría determinar, en su caso, el de la prestación principal"[462].

Según establece el punto 3 de la Recomendación 87/589/CEE:

«a) Los terminales de pago electrónico registrarán, controlarán y transmitirán el pago y podrán integrarse en un terminal de punto de venta

b) Si el prestador así lo desea, podrá tener la posibilidad de dotarse de un único terminal polivalente

c) El prestador tendrá la posibilidad de elegir libremente su terminal de punto de venta, de alquilarlo o comprarlo, con la única condición de que esté autorizado para satisfacer las exigencias del sistema de pago en conjunto y para incorporarse al proceso de interoperabilidad».

El uso correcto de los mencionados medios, en particular de los publicitaros, se concreta también, dentro de la obligación integrativa instrumental, en poner los emblemas y distintivos de los sistemas de tarjeta contratados en sus locales o sitios web en un lugar visible desde el exterior del local comercial y en situar el terminal de modo que permita al titular

[461] *Ibidem,* op., cit., pp. 588 y ss; NUÑEZ LOZANO, P. L.: *Tarjeta de…*op., cit., 246 p; GETE ALONSO Y CALERA, M. *Tarjeta de…*op., cit., p. 100; MARIÑO LÓPEZ, L. *Responsabilidad contractual*…op., cit. p. 129.

[462] SÁNCHEZ GÓMEZ, A. *El sistema de…op., cit.,* pp. 166 y ss.

localizarlo fácilmente para así poder utilizarlo de manera segura, rápida y cómoda[463]. El buen cumplimiento de dichas obligaciones permitirá que la tarjeta sirva como instrumento de pago cuando es presentada por el titular.

Asimismo, la instrucción que deben proporcionar los establecimientos a sus empleados sobre el funcionamiento del sistema de tarjeta contratada, se configura como una obligación integrativa instrumental encaminada a dar cumplimiento a la principal obligación de aceptación de la tarjeta.

Según pone de relieve la doctrina, sería "admisible la responsabilidad del establecimiento por la actuación de sus empleados, si estos no aceptan la tarjeta teniendo obligación de hacerlo, o las aceptan sin hacer las verificaciones pertinentes produciéndose perjuicios para el verdadero titular, en el caso de que resulte que no sea éste quien haya realizado la transacción"[464]. El cumplimiento de estas obligaciones es previo a la realización del contrato de cambio con el titular.

Es una obligación esencial ya que de ella depende el éxito o fracaso del pago con tarjeta[465]. El aceptante puede rechazar la tarjeta cuando no se cumplan los requisitos de admisión que el adquirente haya hecho constar. Y si a pesar de que concurra una causa de rechazo de la tarjeta, ésta es aceptada, asume entonces el riesgo de que la operación sea aceptada o no por el adquirente y, en última instancia, por el titular.

La Disposición Complementaria IV. 3 de la Recomendación 87/598 UE alude a lo relativo a las relaciones entre los prestadores y los consumidores, estableciendo que «el prestador escribirá en forma perfectamente visible las

[463] BOQUERA MATARREDONA, J. "El impago de…", *op., cit*., p. 392; SÁNCHEZ GÓMEZ, A. *El sistema de…op., cit.,* p. 167.

[464] SÁNCHEZ GÓMEZ, A. *El sistema de…*op., cit., p.167. vid. La SAP de Orense de noviembre de 2003(*JUR* 2004, 16246).

[465] BARUTEL MANAUT, C, *Las tarjetas de*…op., cit., pp. 592 y ss.

tarjetas o las siglas de las tarjetas objeto de su afiliación y que esté obligado a aceptar».

3. Obligación de verificar la tarjeta

Es una obligación de protección derivada de la buena fe que adquiere su capacidad en el momento de realización del contrato de cambio con el titular; es decir a través de esta obligación el proveedor debe verificar los datos subjetivos y objetivos de la tarjeta.

En el ámbito objetivo[466], la primera de las verificaciones que debe hacer el establecimiento es comprobar que la tarjeta pertenece al sistema al cual está adherida. Teniendo en cuenta la firma de un contrato de aceptación o admisión de tarjeta entre emisor y el establecimiento, éste último viene obligado a admitir como medio de pago cualquiera tarjeta perteneciente al sistema, por lo que el emisor estaría obligado a realizar al establecimiento los pagos ordenados por los titulares de las tarjetas[467].

En segundo lugar, el establecimiento tiene la obligación de asegurarse de que la tarjeta no esté alterada o manipulada[468]. Por medio de dicha exigencia se procura evitar el uso indebido de la tarjeta, ya sea por su titular o por un tercero no autorizado[469].

[466] Véanse, NUÑEZ LOZANO, P. L.: *Tarjeta de…*op., cit., 246 p; MARIÑO LÓPEZ, A. *Uso fraudulento de*…op., cit., p. 137.
[467] NUÑEZ LOZANO, P. L.: *Tarjeta de…*op., cit., p. 246.
[468] GETE ALONSO Y CALERA, M. C. *Tarjeta de*…op., cit., pp.100; NUÑEZ LOZANO, P. L. *Tarjeta de*…op., cit., pp. 246 y ss; BARUTEL MANAUT, C. *Las tarjetas de*…op., cit., pp. 594; STS, de 3 de diciembre de 1991; MARIÑO LÓPEZ, A. *Uso fraudulento de*…op., cit., p. 137;
[469] Vid. NUÑEZ LOZANO, P. L.: *Tarjeta de…*op., cit., p. 246.

En tercer lugar, le corresponde al establecimiento verificar si la tarjeta[470] no está caducada o vencida, así como también consultar si la tarjeta presentada no ha sido anulada o cancelada.

Teniendo en cuenta el criterio subjetivo, el establecimiento adherido al sistema debe verificar si existe coincidencia entre la personalidad de quien pretende utilizar la tarjeta y la persona nominalmente designada en la misma[471].

La necesidad de esta verificación es sólo para aquellos casos en que el cotejo entre las firmas estampadas en la tarjeta y en la factura o nota de cargo correspondiente a la operación instrumentada muestre indicio de que existe diferencia entre ellas; es decir en caso de duda "el establecimiento procederá a la comprobación de la autenticidad de la firma haciendo que el titular de la tarjeta firma la nota de cargo y así cotejar la firma con la existente en la tarjeta; si se observan disconformidades entre las dos firmas contrastadas, deberá pedirse al titular un documento que acredite su

[470] Ibídem.

[471] Véanse, FARRANDO MIGUEL, I y CASTAÑER CODINA, J.: "Atribución y…*op., cit*., pp. 87 y ss.; NÚÑEZ LOZANO, P.L., señala que cuando le sea presentada una tarjeta de las reguladas en este contrato, el establecimiento adherido deberá comprobar la identificación del titular mediante DNI, NIF o Pasaporte, y que coincide la firma estampada por el cliente en la factura con la firma de la tarjeta, en NÚÑEZ LOZANO, P.L. *La tarjeta...*op., cit., p. 247; sobre este mismo aspecto véanse MARIÑO LOPEZ, Andrés. *Uso fraudulento de tarjetas de crédito por terceros no autorizados. Daños y responsabilidad civil.* Prólogo de Santiago Herrero Anibarro. Madrid: Marcial Pons, 2006, pp.135 y ss; GETE ALONSO Y CALERA, M. C. *Tarjeta de*… op., cit., pp.100 -101; BAUTECAS CALETRIO, A. *Pago con*…op., cit., p. 284. Según establece la SAP de Baleares, (sección 5.ª), de 26 de febrero de 1997, ...en una relación en la que aparte de ventajas para propio titular, reporta beneficio económico a la entidad emisora y al comerciante, y así el titular puede legítimamente esperar que los demás intervinientes (entidad emisora y establecimiento asociado) conocedores de la calidad de personal intransferible de la tarjeta se cerciorarán de la identidad de los usuarios, comprobarán a la autenticidad de la firma, y en su caso. Solicitarán la exhibición de la oportuna documentación acreditativa, y en tal sentido en el clausulado del contrato de tarjetas se recoge la obligación del titular de la tarjeta si así se le exige tras haber firmado el correspondiente recibo, sin que deba responder por el fallo de sistema del cual es ajeno".

personalidad y, en caso de duda, consultar a su entidad emisora"[472]. Sólo así se podrá detectar el uso indebido de la tarjeta por tercero no autorizado.

Existen criterio de quienes señalan que, "si se emplea la tarjeta a través de un mecanismo electrónico de registro y transmisión de datos, mediante un terminal de punto de venta (TPV) idóneo para procesar los datos que consten en la banda magnética inserta en el documento, entonces algunas de las verificaciones mencionadas con anterioridad, sin perjuicio de que el establecimiento adherido al sistema tenga de igual manera que efectuarlas personalmente, se harán de forma electrónica (cuando se presenta la tarjeta el establecimiento deberá pasarla por el lector de TPV y pulsar los datos y realizar las operaciones que sean de aplicación)" [473].

Como ya hemos señalado a lo largo de esta investigación, en el comercio electrónico la utilización de la tarjeta de pago es puramente «virtual», ya que la tarjeta no se exhibe ante el establecimiento o proveedor de bienes o servicios. Por lo que el proveedor de bienes o servicios no podrá verificar la verdadera identidad de quien presenta la tarjeta; tampoco puede comprobar la firma de la tarjeta y ni siquiera puede exigir conocimiento de una clave secreta asociada a la tarjeta[474]. Al no existir la nota de cargo que el

[472] NUÑEZ LOZANO, P. L. *Tarjeta de…op., cit.,* p. 248; MARIÑO LÓPEZ, A. *Uso fraudulento de*…op., cit., p.143; vid. SAP Madrid (Sección 18º), de 29 de julio de 1998; BARUTEL MANAUT, C. *Las tarjetas de*…*op., cit*., pp. 594 y ss.

[473] NUÑEZ LOZANO, P. L. *Tarjeta de…op., cit*., pp. 24; según señala MARIÑO LÓPEZ, Andrés. *Uso fraudulento de…*op., cit., p. 143, el establecimiento "no puede comprobar, al momento de aceptar el pago con tarjeta de crédito, los diversos aspectos que indican que admite una operación valida: el estado de la tarjeta; su límite temporal y/o crédito; coincidencia de las firmas de nota de cargo o cupón con la que luce en la tarjeta; identificación del titular de la tarjeta por su documento de identidad". Este mismo autor, apunta que, "no obstante, el establecimiento adherido tiene a su cargo obligaciones específicas para controlar el pago con tarjeta de crédito en la contratación a distancia que le son atribuidas en el contrato de aceptación. En efecto, al momento de aceptar el pago con dicho documento de pago, el establecimiento adherido debe realizar la consulta respectiva a la entidad emisora. De esta forma cumple con una de las conductas que debe desarrollar para dar cumplimiento a su obligación de verificación".

[474] Vid. MARTÍNEZ NADAL, «Atribución de responsabilidad al comerciante o a la entidad bancaria», p. 218; GUIMARÃES, M. R. "El pago...", *op., cit*., p. 172; MARIMÓN DURÁ, R. *La tutela del…op., cit.*, p. 221

establecimiento presenta al emisor para obtener el pago de la operación realizada, aquel no podrá verificar su autenticidad. Es decir, el establecimiento se encuentra imposibilitado para verificar directamente los datos objetivos y subjetivos de la tarjeta[475]. A pesar de esto, el pago mediante dispositivo electrónico puede ser acreditado mediante la certificación de los asientos en la cuenta corriente bancaria del cliente y del establecimiento[476].

Se ha de resaltar que para comprobar la validez de la tarjeta se utilizan pasarelas de pago que son instaladas por el emisor y gestionadas por él mismo o por un tercero. El mecanismo de la pasarela de pagos sólo permite la verificación técnica del instrumento de pago (que no esté vencido, anulado o que la operación no exceda del límite de crédito autorizado). El sistema no puede garantizar que sea el propio titular quien está efectuando la operación. Según sostiene algún autor "en estos casos, la responsabilidad del emisor se circunscribe al funcionamiento técnico de la pasarela de pagos, sin responder de la identidad del sujeto que está utilizando la tarjeta. Estas circunstancia debe estar especificada en los contratos de afiliación, aquí nos encontramos con un ejemplo de delimitación del riesgo, el emisor, al exonerarse de responsabilidad por la verificación de la identidad del titular traslada el riesgo de las operaciones fraudulentas al aceptante"[477].

[475] MARIÑO LÓPEZ, Andrés. *Uso fraudulento de…op., cit.,* pp.148 y ss.

[476] Vid. RICO CARRILLO, M. *Comercio...*op., cit., p. 177, según esta autora la facturación viene siendo uno de los mecanismos más idóneos para comprobar el pago efectuado a través de medios electrónicos, se basa en el sistema de "facturación electrónica"; además sostiene esta autora en uno de sus obras publicadas, que "para verificar la identidad del titular se utilizan mecanismos basados en el suministro de claves personales y códigos de seguridad asociados al instrumento de pago, también los protocolos de seguridad descritos anteriormente y, en menor medida, firmas electrónicas basadas en criptografía de clave pública".

[477] MARIÑO LOPEZ, A*. Uso fraudulento de…*op., cit., p. 149.

4. Obligación de entregar al titular un comprobante de la operación

Según lo establecido en el art.6.3 de la Recomendación 88/590/CEE, «se facilitará al titular, cuando así lo solicite, un extracto de sus operaciones, inmediatamente o poco después de su realización; no obstante, cuando se trate de un pago en el punto de venta, el recibo de caja facilitado por el detallista en el momento de la compra, y que contendrá las referencias al instrumento de pago deberá reunir los requisitos de la presente disposición». Igualmente se recogen estas obligaciones en el art. 10.1b) de la LGDCU.

Los establecimientos comerciales facilitan dos comprobantes: el tique de compra o la factura, y la nota de cargo que cumple con los requisitos establecidos en la Recomendación que acabamos de examinar[478]. Por último, cabe señalar que esta obligación surge una vez que se celebra el contrato de cambio y el establecimiento realiza las verificaciones pertinentes y acepta la tarjeta como medio de pago, por lo que éste deberá entregar un comprobante de la operación efectuada por el titular[479].

5. Obligación de conservar el ejemplar original de las facturas de venta o notas de abono durante el plazo mínimo estipulado en el contrato

La finalidad que persigue esta obligación es la de contar con un medio de prueba que sirva de justificación de la venta o servicio prestado y que permita resolver las futuras reclamaciones, tanto de la parte emisora como del titular de la tarjeta[480]. Al igual que en el "comercio tradicional", en el comercio electrónico el proveedor de bienes o servicios tiene la misma obligación de conservar las facturas de venta en un formato electrónico para que sirvan de medio de prueba. En el caso de que éste no haya guardado

[478] BARUTEL MANAUT, C, *Las tarjetas de*…op., cit., pp. 611-612.
[479] SÁNCHEZ GÓMEZ, A. *El sistema de*…op., cit., p. 178; BATUECAS CALETRIO, A. *Pago con…*op., cit., pp. 282 y ss.
[480] GETE ALONSO Y CALERA, M. C. *Las tarjetas de…*op., cit., p. 100; LAFUENTE SÁNCHEZ, R. *Los servicios financieros*…op., cit., p. 256; BATUECAS CALETRIO, A.: *Pago con…op., cit.,* pp. 282 y ss.

dichas facturas, asumirá los perjuicios y daños derivados de la negativa por parte del titular a asumir los cargos correspondientes.

También le incumbe al proveedor de bienes o servicios la obligación de satisfacer las cuotas, comisiones, gastos e impuestos por razón del contrato pactado.

Por último, se ha de concluir que el proveedor de bienes o servicios tiene que mostrar al cliente información sobre el tratamiento que tendrán sus datos personales para que el usuario decida si desea facilitar estos datos. Asimismo debe tener registrado el fichero de datos en la Agencia Española de Protección de Datos que obliga además a elaborar un documento de seguridad que garantice la seguridad de esos datos. También debe enseñar claramente los datos identificativos y fiscales del titular (propietario), incluyendo el NIF/CIF, nombre de la empresa, datos de contacto, registro mercantil (si fuera aplicable). De tal forma que el cliente pueda saber realmente dónde compra y a quién tiene que reclamar en caso de cualquier problema[481].

Además, le concierne al proveedor de bienes o servicios en el comercio electrónico, la obligación de informar al consumidor del precio total de la adquisición del bien o servicio, "indicando de manera diferenciada el precio del producto y el importe de los incrementos o descuentos en su caso y de los costes adicionales por servicios, accesorios, financiación, aplazamiento o similares"[482].

[481] Vid., art. 6.1, a), b), c)…, Directiva 2011/83/UE

[482] SAP de Burgos (Sección 3ª), de 16 de julio de 2007) JUR\2007\320933. A su vez esta información, cuando se incorpora a una oferta de contrato, es vinculante para el empresario y puede ser exigida por el consumidor al amparo de lo dispuesto en el artículo 8.1 de la LGDCU; según se prevé en el Considerando (38) de la Directiva de 2011/83/CE, Los sitios web de comercio deben indicar de modo claro y legible, a más tardar al inicio del procedimiento de compra, si se aplica alguna restricción de suministro y cuáles son las modalidades de pago que se aceptan.

Por su parte, el artículo 8 de la Directiva 2011/83/UE establece que corresponde al comerciante (proveedor de bienes o servicios) facilitar al consumidor la confirmación del contrato en un soporte duradero y en un plazo razonable después de la celebración del contrato a distancia, a más tardar en el momento de entrega de los bienes o antes del inicio de la ejecución del servicio.

Tal confirmación incluirá: a) toda la información que figura en el artículo 6, apartado 1, salvo si el comerciante ya ha facilitado la información al consumidor en un soporte duradero antes de la celebración del contrato a distancia; y b) cuando proceda, la confirmación del previo consentimiento expreso del consumidor y del conocimiento por su parte de la pérdida del derecho de desistimiento de conformidad con el artículo 16, letra m)"[483].

3.5.4. Obligaciones y carga de la entidad adquirente

a) Obligación de facilitar el soporte material y técnico al establecimiento

Nos habíamos referido con anterioridad la obligación del proveedor de bienes o servicios adherido de contar con adecuados medios tecnológicos, materiales y publicitarios. En este apartado se hará referencia a la obligación del adquirente de facilitar al aceptante a título de depósito el material

[483] Por su parte, el art. 6.1 de la Ley 22/ 2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores(LCDSFDC), establece que, «por soporte duradero se entiende todo instrumento que permita al consumidor almacenar la información dirigida personalmente a él, de modo que pueda recuperarla fácilmente durante un período de tiempo adecuado para los fines para los que la información está destinada y que permita la reproducción sin cambios de la información almacenada»; en este sentido, RODRÍGUEZ DE LAS HERAS BALLELL, sostiene que el "soporte digital o electrónico, se puede definirse "como todo material, dispositivo o instrumento que sirva para volcar, guardar, almacenar o dejar constancia de una información en dígitos", RODRÍGUEZ DE LAS HERAS BALLELL, T. "Reparto del riesgo..."*op., cit.,* p. 320, nota 8; por su parte, el art. 2. 10 de la Directiva 2011/83/UE, define el «soporte duradero»: "todo instrumento que permita al consumidor o al comerciante almacenar información que se le transmita personalmente de forma que en el futuro pueda recuperarla fácilmente durante un período de tiempo acorde con los fines de dicha información y que permita la reproducción de la información almacenada sin cambios".

necesario para la tramitación de las operaciones con tarjeta, tales como impresos manuales, adhesivos publicitarios o pl aca de identificación del establecimiento; también puede facilitar el Terminal de punto de venta virtual (TPVs) o Terminal de pago electrónico (TPEs)[484].

La entidad adquirente debe disponer lo necesario para informar al aceptante sobre la vigencia de las tarjetas, tanto las que son anuladas como las denunciadas por cualquier causa[485]. El cumplimiento de esta obligación es fundamental para que el establecimiento adherido al sistema pueda cumplir la obligación de aceptar la tarjeta[486]

b) Obligación de pagar al aceptante el importe de las transacciones

La obligación principal del adquirente es la de pagar al establecimiento o aceptante de l a tarjeta el importe de las transacciones efectuadas por el titular de la tarjeta[487].

c) Obligación de recompensar al aceptante por su colaboración en la lucha contra el fraude en las tarjetas

Es una obligación asumida por el adquirente que aparece en todo el contrato existente entre éste y el aceptante[488]. Por ella, el adquirente se obliga a gratificar al establecimiento adherido al sistema para que colabore en la lucha contra el fraude en el sistema de tarjeta.

[484] BARUTEL MANAUT, C. *Las tarjetas de…op., cit.,* p. 624*;* SÁNCHEZ GÓMEZ, A. *El sistema de*…op., cit., p. 178.
[485] BARUTEL MANAUT, C. *Las tarjetas de…op., cit.,* p. 624*.*
[486] SÁNCHEZ GÓMEZ, A. *El sistema de*…op., cit., p.178.
[487] BARUTEL MANAUT, C, *Las tarjetas de…*op., cit., p. 624; SÁNCHEZ GÓMEZ, A. *El sistema de*…op., cit., p. 178.
[488] BARUTEL MANAUT, Carles, *Las tarjetas de…*op., cit., p. 633*;* SÁNCHEZ GÓMEZ, A. *El sistema de*…op., cit., p.195.

Cabe señalar que la doctrina se ha demostrado preocupada sobre la naturaleza jurídica de este pago[489]. En este sentido, se plantea que se trata de una donación hecha al aceptante por su lucha contra el fraude en el sistema de pago con tarjeta[490].

Finalmente conviene señalar que dicha obligación viene siendo como la contraprestación consistente en una cantidad de dinero que asume el adquirente por el servicio realizado por el aceptante, que consiste en la lucha contra el fraude en la utilización de tarjetas[491]. Y por último, siguiendo este criterio, diríamos es una obligación propia de un contrato de servicios[492].

d) Obligación de guardar la debida confidencialidad sobre los datos que obtenga de los titulares y aceptantes

Al igual que la entidad emisora, la entidad adquirente tiene la misma obligación y deber de mantener la confidencialidad sobre los datos del titular y de los aceptantes. La Recomendación 87/598 CE, establece en su punto III.4.b) que «al efectuar el pago, los datos transmitidos al banco del prestador y posteriormente al emisor no afectarán, en ningún caso, a la protección de la vida privada. Se limitarán estrictamente a los datos previstos normalmente para cheques y transferencias». Para garantizar la confidencialidad de las partes intervinientes en la operativa de pago es necesario que la entidad adquiriente cumpla con la obligación de instalar un sistema de pago seguro

[489] Vid. SÁNCHEZ GÓMEZ, A. *El sistema de*…op., cit., p. 195; BARUTEL MANAUT, Carles, *Las tarjetas de…op., cit.,* p. 633.

[490] Según la tesis sostenida por SÁNCHEZ GÓMEZ, "existen obstáculos que plantea esta posición jurídica. Entre ellos podemos mencionar el de la discusión sobre la remuneración de servicios futuros, que contemplan las condiciones generales. Y por último, que en el contrato de afiliación existe, más que una remuneración, una promesa o compromiso de donación remuneratoria por los servicios prestados por el aceptante", en SÁNCHEZ GÓMEZ, A.: *El sistema de*…op., cit., p. 195.

[491] véanse BARUTEL MANAUT, C. *Las tarjetas de…*op., cit., pp. 633 y 634*;* SÁNCHEZ GÓMEZ, A. *El sistema de*…op., cit., p. 196.

[492] SÁNCHEZ GÓMEZ, A. *El sistema de…op., cit.,* p.196.

Pues bien, se ha señalado por la doctrina que los contratos no recogen esta obligación; sin embargo, se considera como una cláusula que perjudica a todos los emisores[493].

3.6. Obligaciones de algunos intermediarios en el sistema de pago electrónico mediante tarjeta

3.6.1. Obligaciones del proveedor de acceso a Internet

Una de las obligaciones que asume el proveedor de acceso o servidor frente al usuario, es la de prestar un servicio de conexión a Internet por un determinado periodo de tiempo. El proveedor tiene la obligación de facilitar al usuario claves de identificación (logging y un password) que permita el acceso al servicio[494].

Además, le corresponde la obligación de informar sobre el funcionamiento del sistema para que el usuario pueda acceder a la información[495]; es decir los proveedores de servicios de acceso a Internet estarán obligados a informar a sus clientes, en los términos que se establezca reglamentariamente, de forma permanente, fácil, directa y gratuita, sobre los medios técnicos que permitan, entre otros, la protección frente a virus informáticos y programas espía, la restricción de los correos electrónicos no solicitados, y la restricción o selección del acceso a

[493] Como indica BARUTEL MANAUT, Carles, *Las tarjetas de…*op., cit., pp. 635 y ss, el emisor no sólo tiene el deber de confidencialidad por su actuación antes los titulares y los aceptantes, sino que igualmente se extiende a la actuación del aceptante frente a los titulares. Sobre este mismo se señaló también, que el adquirente debe trasladar su obligación de confidencialidad sobre los aceptantes, extremo que no se halla habitualmente contemplado en los contratos.

[494] Véanse GARCÍA VIDAL, Ángel. "Contratos de acceso. El acceso al comercio electrónico.", en GÓMEZ SEGADE, J.A (coord.). *Comercio electrónico en Internet.* Madrid: Marcial Pons, 2001, p.112; RICO CARRILLO. M. «Responsabilidad civil de los…» *op., cit*., p.3.

[495] HERNANDO, Il. *Contratos..op., cit.,* pp. 717 y ss.

determinados contenidos y servicios ilícitos o nocivos para la juventud y la infancia (art.12.1bis de la LMISI)[496].

Al mismo tiempo, se le obliga a informar a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial (art.12.4 bis de la LMISI).

El proveedor de acceso a la red se encuentra obligado también a mantener en secreto el contenido de la información que reciba o envíe al usuario, en el sentido de que dicha información no llegue a manos de un tercero no autorizado que podría utilizarla con fines fraudulentos.

3.6.2. Obligaciones del usuario

El usuario está obligado hacer un buen uso de su login y contraseña, pues ambos son personales e intransferibles. No podrá darlos a conocer a terceras personas y, en el caso que ocurran circunstancias no previstas, deberá comunicarlo urgentemente al proveedor.

3.6.3. Obligaciones de los prestadores de servicios de certificación

Antes de abordar cuestiones relacionadas con las obligaciones de los prestadores de servicios de certificación, creemos que es necesario recalcar que en la operativa de pago con tarjeta en el comercio electrónico seguro a través de Internet, el proveedor de servicios de certificación desempeña la función de "tercera parte de confianza" que media entre cliente y proveedor de bienes o servicios con el fin de garantizar la identidad de las partes (art.25 LSSICE)[497]. Es decir, "se trata de un tercero que intermedia en la

[496] España: Ley 56/2007.
Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. (*BOE*, núm. 312, de 29 de diciembre de 2007).

[497] Esta ley fue modificada por la Ley 56/2007, de 28 de diciembre, de Medida de

comunicación certificando claves, validando fecha, hora y lugar, encriptando el documento electrónico con sus claves privadas para luego enviarlo a las partes quienes desencriptarán con la clave pública, posibilitando la prueba de la notificación, autoría, no repudio, autentificación, integridad, etc…"[498].

Como señalan algunos autores, en el caso de los pagos efectuados mediante tarjetas electrónicas, el proveedor de servicios de certificación mantiene una relación contractual principalmente con el emisor que es la que verifica el sistema que autoriza el pago con tarjeta; no obstante eso no influye para que el titular de la tarjeta también pueda acceder a los servicios que presta esta entidad, solicitando su par de claves con el fin de asegurar su intervención en el comercio electrónico, mediante el cifrado de su mensaje[499].

En el Derecho español, la Ley 59/ 2003, de 19 de diciembre, de firma electrónica establece dos tipos de obligaciones: la primera se refiere a las obligaciones exigibles a cualquiera de los prestadores de servicios de certificación que expidan certificados electrónicos, ya sea reconocidos o no; y la segunda se refiere a las obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos reconocidos. Por lo tanto, es importante distinguir cada una de estas obligaciones. Antes de analizar estas dos obligaciones, lo primero que haremos es examinar las obligaciones exigibles a los prestadores de servicios de certificación que expiden certificados reconocidos (art.12 LFE).

Impulso de la Sociedad de la Información (*BOE*, núm. 312, de 29 de diciembre de 2007); así, la Profesora RODRÍGUEZ DE LAS HERAS BALLEL sostiene que los terceros de confianza " actúan como intermediarios reputacionales o de confianza, sobre la base del valor añadido implícito en la información que suministran con la consiguiente reducción en el coste de recopilación y verificación, por razón de su credibilidad", RODRÍGUEZ DE LAS HERAS BALLELL, T; ALBA FERNÁNDEZ, M. «Las agencias de rating*…» op., cit*., p. 150.

[498] RICO CARRILLO. M. «Responsabilidad civil de los…» *op., cit*., p. 5.

[499] Ibídem, p.5.

3.6.3.1. *Obligaciones exigibles a los prestadores de servicios de certificación que expiden certificados reconocidos*

Un prestador de servicios de certificación antes de expedir un certificado reconocido lo primero que debe hacer es cumplir con las obligaciones establecidas en el art. 12 de la LFE, que son:

« a) Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente

b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido

c) Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado

d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación».

3.6.3.2. *Obligaciones de los prestadores de servicios de certificación que expiden certificados electrónicos*

Según se establece en el inciso a) del art. 18 de la LFE, los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones[500]:

[500] Igualmente, la Ley Modelo CNUDMI sobre firma electrónica, hace referencia expresa a las obligaciones de los prestadores de servicios de certificación, en su art.9 con el título "Proceder del prestador de servicios de certificación" , prevé en el apartado 1 que «cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica

«a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios».

Es decir, se trata de una medida de seguridad básica que garantiza que sólo el titular de la firma va tener acceso a los datos de creación de firma, por lo que es importante que la firma sea avanzada[501]. En este sentido, hay quienes indican que "ni siquiera por error de la entidad certificadora o fraude de terceros, y salvo en el momento de generación de las claves, podrá

---

que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;

c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) Proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

i) el método utilizado para comprobar la identidad del firmante;

ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8 de la presente Ley; vi) si se ofrece un servicio para revocar oportunamente el certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que existe un servicio para revocar oportunamente el certificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables".

Y por último establece en su apartado 2 "Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1".

[501] CRUZ RIVERO, A*.: La firma electrónica reconocida. Análisis de los requisitos del artículo 3.3 de la Ley 59/2002, de 19 de diciembre, de firma electrónica.* Madrid: Consejo General del Notariado, 2006, p. 105; vid. ILLESCAS ORTIZ, R.: *Derecho de la contratación...op., cit.,* p. 138.

acceder un tercero a los datos de creación de firma. Por lo tanto, puede afirmarse que si un tercero llega a tener conocimiento de los datos de creación de firma habrá sido a partir del propio firmante, custodia de las claves"[502].

Según algunos autores es de destacar el cambio que ha supuesto esta disposición respecto del Real Decreto Ley 14/1999 de firma electrónica (derogado) en cuyo art. 11.c) se imponía a todas las entidades de certificación el deber de «no almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que esta lo solicite»[503]. Por esta razón, se permitía que el solicitante de la firma pidiera al prestador de servicios de certificación que custodiara también los datos de creación de firma, lo que, en caso de pérdida, serviría para no tener que generar un nuevo par de claves.

Sin embargo, la actual LFE establece que no pueden existir duplicados de claves privadas ya que los datos de creación de firma son datos únicos, como códigos o claves criptográficas privadas, que el prestador utiliza para crear la firma electrónica, por lo que tienen que estar bajo su custodia y nadie puede tener acceso a ellos; por tal razón, cuando se generen datos de creación de firma, los prestadores de servicios de certificación no podrán almacenarlos ni copiarlos[504]. Si el titular entrega la clave a un tercero lo hará bajo su responsabilidad.

Además, el literal b) de este mismo artículo establece la obligación del prestador de servicios de certificación de «proporcionar al solicitante, antes de la expedición del certificado, la siguiente información mínima que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

[502] CRUZ RIVERO, A*.: La firma electrónica...,* op., cit., p. 105.
[503] *Ibídem,* p.105.
[504] Vid. DAVARA RODRÍGUEZ, M.A. *La seguridad…, op., cit.,* p. 77.

1. Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido

2. Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo

3. El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado

4. Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial

5. Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad

6. Las demás informaciones contenidas en la declaración de prácticas de certificación».

Por su puesto, se trata de una obligación de informar que se le debe proporcionar al solicitante del certificado de forma gratuita, ya sea por escrito o en forma electrónica, sobre cómo se debe utilizar la firma y el certificado[505]. Además, se señala, que "la información citada anteriormente

[505] En opinión de CRUZ RIVERO, el inciso k) de ANEXO II DFE, alude a que los prestadores de servicios de certificación que expidan certificados reconocidos deben «antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio

que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos".

Por su parte, el literal c) art.18 de la LFE se establece que el prestador de servicios de certificación tiene la obligación de «mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados». Mientras que en el Real Decreto Ley (derogado) se utilizaba la terminología de un "registro de certificado" en lugar de "directorio" quizás porque para el legislador la expresión registro debía ser empleado en otro contexto.

Respecto de la obligación de mantener un directorio actualizado de certificados, algunos autores consideran que "se trata de una garantía en la que se persigue que se proporcione la seguridad a la firma electrónica una vez que se mantiene un directorio de certificado se puede comprobar su existencia, vigencia o si ésta ha sido suspendida o extinguida. De acuerdo al interés de estos directorios para garantizar la seguridad jurídica de la firma electrónica, se exige también que la integridad del directorio se proteja mediante la utilización de mecanismos de seguridad"[506].

Y como última obligación recogida en el art. 18, d) de la LFE los prestadores de servicios de certificación que expiden certificados electrónicos deben «garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro».

---

de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado», CRUZ RIVERO, A.: *La firma electrónica...*op., cit., p.108**,** nota al pie 264.

[506] Vid. DAVARA RODRÍGUEZ, M.A. *La seguridad…op., cit.,* p. 78.

3.6.3.3. *Obligaciones de los prestadores de servicios de certificación que expiden certificados electrónicos reconocidos*

El art.20.1 de la LFE señala que además de las obligaciones establecidas en el art. 18 de la misma Ley, los prestadores de servicios de certificación que expidan certificados reconocidos deben cumplir las siguientes obligaciones[507]:

[507] Del mismo modo, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1 999, por la que se establece un marco comunitario para la firma electrónica, establece en su anexo II, los requisitos de los Proveedores de servicios de certificación que expiden certificados reconocidos, señalando que estos deberán:

«a) demostrar la fiabilidad necesaria para prestar servicios de certificación;

b) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;

c) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;

d) comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;

e) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas;

f) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;

g) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos;

h) disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado;

i) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;

j) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves;

k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de

« a) Demostrar la fiabilidad necesaria para prestar servicios de certificación

b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia

c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica

d) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte

e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante

f) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo

---

dicha información estarán también disponibles a instancias de terceros afectados por el certificado;

l) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:- sólo personas autorizadas puedan hacer anotaciones y modificaciones, -pueda comprobarse la autenticidad de la información-, los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado, y - el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados».

g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad».

2 Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000€ para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan. La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000€.

3.7. Consideraciones finales

Tras examinar a lo largo de este capítulo, las distintas obligaciones y cargas de los sujetos intervinientes en los distintos contratos de tarjeta de pago (crédito), hemos llegado a las siguientes conclusiones:

En primer lugar, se ha de señalar que en el contrato de emisión de tarjeta suscrito entre la entidad emisora y el titular de la tarjeta se establecen lógicamente una serie de obligaciones para ambas partes. Por medio de este contrato la entidad emisora o gestora se obliga a:

- emitir la tarjeta de pago, así como gestionarlo como medio de pago, ya sea, “on line u off line”
- adoptar todas las medidas pertinentes de seguridad necesaria para garantizar el buen funcionamiento de su sistema e impedir la utilización fraudulenta del mismo tanto por su titular como por tercero no autorizados.

- informar al titular de las medidas de seguridad en Internet; suministrar la información sobre el funcionamiento del sistema de pago y el registro de las operaciones realizadas por el titular de la tarjeta a través del sitio web de la entidad o mediante el envío de un extracto por correo electrónico

- mantener en secreto los datos confidenciales del titular (NIP o el código secreto), para que estos no puedan ser interceptados por un tercero ajeno al contrato de emisión de la tarjeta, y que después lo utilice fraudulentamente

- garantizar la disponibilidad de un sistema o medio adecuado y gratuito que permita al cliente comunicar o notificar la pérdida, sustracción o el extravío de la tarjeta mediante el bloqueo de las operaciones de pago

- facilitar gratuitamente al usuario o el titular de la tarjeta medios que permitan demostrar que ha efectuado dicha comunicación.

Las obligaciones del titular de la tarjeta tras firmar el contrato de emisión son las siguientes:

- hacer un uso correcto y adecuado de la tarjeta, así como garantizar la seguridad de la misma

- custodiar la tarjeta y a mantener en secreto el NIP

- comunicar o notificar sin "demora indebida" a la entidad emisora el extravío o sustracción de la tarjeta

En segundo lugar cabe concluir que en el contrato de aceptación, adhesión o de pasarela de pago al sistema de tarjeta celebrado entre la entidad emisora de la tarjeta y/o gestor y el proveedor de bienes o servicios,

se establecen cargas y obligaciones de las partes contratantes. Mediante este contrato la entidad emisora se obliga frente al proveedor de bienes o servicios a:

- pagar las facturas firmadas por el titular
- Instalar los dispositivos técnicos que permite gestionar la autorización de la transacción, mediante pasarela de pago virtual o terminal de punto de venta virtual (TPVS).

Por su parte el proveedor de bienes o servicios adherido al sistema tiene como obligaciones:

- Aceptar la tarjeta como medio de pago en aquellas transacciones efectuadas por el titular de la tarjeta
- Verificar los datos subjetivos u objetivos de la tarjeta de pago. En el comercio electrónico la utilización de la tarjeta es puramente virtual, por lo que el proveedor de bienes o servicios no podrá comprobar, al momento de aceptar el pago con tarjeta, los diversos requisitos que indican que admite una operación valida: identificación del titular y coincidencia de las firmas de nota de cargo, entre otros.
- En el momento de aceptar el pago mediante tarjeta, el proveedor de bienes o servicios debe realizar la consulta respectiva a la entidad emisora. De esta forma cumple con una de las conductas que debe desarrollar para dar cumplimiento a su obligación de verificación.

Universidad
Carlos III de Madrid

CAPÍTULO CUARTO

EL REPARTO DE RIESGOS Y LA ATRIBUCIÓN DE RESPONSABILIDAD CIVIL POR EL USO FRAUDULENTO DE TARJETA EN EL COMERCIO ELECTRÓNICO

CAPÍTULO IV.

EL REPARTO DE RIESGOS Y LA ATRIBUCIÓN DE RESPONSABILIDAD POR EL USO FRAUDULENTO DE TARJETA EN EL COMERCIO ELECTRÓNICO

4. INTRODUCCIÓN

Antes de acometer el análisis de la atribución de la responsabilidad a los sujetos intervinientes en la operativa de pago mediante el uso de la tarjeta de crédito en el comercio electrónico, se hace necesario plantearse los siguientes interrogantes: ¿cómo comienza la operativa del pago con tarjeta en el comercio electrónico?, ¿qué riesgos implica el uso de la tarjeta en el comercio electrónico?

Sobre el primer interrogante cabe resaltar que la operativa del pago con tarjeta en el comercio electrónico comienza de la siguiente forma: el cliente hace el pedido proporcionando los datos necesarios--generalmente el número de tarjeta, la fecha de caducidad, el código de seguridad (CVV2)--al proveedor de bienes o servicios a través de un canal seguro como es el proporcionado por el sistema SSL comentado en el Capítulo II, que cifra los datos intercambiados entre el servidor del proveedor de bienes y el cliente con un algoritmo de clave simétrico. A su vez el proveedor de bienes o servicios gestionará el pago con el banco mediante las vías tradicionales[508].

También se puede hablar de la operativa de pago mediante tarjetas con el uso de protocolo SET en el comercio electrónico[509], en el que el consumidor realiza un pedido y entonces espera la firma digital del

[508] PANIZA FULLANA, A. *Contratación a distancia…*op., cit., p. 315.
[509] FERNÁNDEZ PÉREZ, N.: *El nuevo régimen…op., cit.,* p.363.

proveedor de bienes o servicios. Una vez comprobada la validez de dicha firma, el consumidor envía el pedido, la orden de pago y la de compra. Toda esta información debe ir acompañada de una firma digital del consumidor o cliente, en el sentido de impedir que dicha información pueda ser interceptada o leída por un tercero no autorizado.

Por otro lado, cabe señalar que una vez que el proveedor de bienes o servicios recibe el pedido de la compra, lo primero que debe hacer es verificar la firma digital del consumidor, y, a su vez, enviar directamente la información del pago (datos de tarjeta) a la "pasarela de pagos", cuya función es procesar los pagos con el objetivo de obtener la autorización o el rechazo de la transacción.

Sobre el segundo interrogante, hemos de reiterar que existe la posibilidad de que los datos enviados pueden ser interceptados por un tercero ajeno a la comunicación, lo que representa un alto grado de inseguridad en las transacciones electrónicas realizadas con tarjeta de pago en Internet. Es decir, en un entorno abierto como Internet, existe el riesgo de que cualquier persona pueda pinchar la red e interceptar los datos de la tarjeta[510].

[510] En la doctrina, MARTÍNEZ NADAL, pone de manifiesto que "el titular de una tarjeta de pago se muestra, en muchos casos reticente a enviar su número de identificación de tarjeta por la red para que le sea cargado, el precio de una compra por diversas razones: ya que el uso abierto de Internet puede ser interceptado por terceros(intercepción que puede ocurrir no sólo en tránsito sino también en destino, una vez que los datos de la tarjetas están en manos del vendedor), la falta de conocimiento directo, por parte del comprador, del comerciante(en cuyas manos se pone una información sensible, lo cual puede dar lugar a usos fraudulentos, intencionados, dolosos directamente por parte del vendedor, o por negligencia en la custodia que permite el acceso no autorizado por parte de terceros)" en MARTÍNEZ NADAL, A. El dinero electrónico…*op., cit.,* pp.18 y ss; siguiéndonos la tesis sostenida por MARTÍNEZ GONZÁLEZ, "los riesgos pueden variar de un medio de pago a otro, también puede darse en función de soporte tecnológico o soluciones tecnológico utilizada en su gravedad; y que los riesgos más común en los pagos electrónicos proviene del hecho en que una persona malintencionado suplante alguno de los participantes en una transacción y de los datos confidenciales accesibles a estafadores por falta o mala protección del sistema que almacena los datos o canal de comunicación utilizada durante la transacción. Y este autor señala que los riesgos pueden ser: a) suplantación del comprador

También puede ser el propio titular de la tarjeta el que actúe de forma negligente, comunicando a un tercero sus datos bancarios. En este sentido, algunos autores sostienen, que "en la contratación a distancia –en la cual los pagos se efectúan generalmente por medio de tarjeta de crédito- se multiplica los riesgos de utilización indebida de instrumento por un tercero no autorizado. A los riesgos que surgen de la imposibilidad de verificación y control por parte del establecimiento adherido de la operación de pago se suma la posibilidad que los signos de individualización de la tarjeta y los documentos que permiten identificar a su titular sean interceptados por un tercero que los utilice en su provecho en forma ilegítima"[511].

En base a eso, hemos de señalar que el objetivo general de este capítulo es determinar la atribución de responsabilidad entre los sujetos intervinientes en el uso de tarjetas en el comercio electrónico. Al mismo tiempo, estudiaremos la cuestión relacionada con las cláusulas de exoneración de la responsabilidad de las partes intervinientes en el sistema de pago electrónico, así como las cláusulas abusivas aplicadas por las entidades emisoras y la nulidad de dichas cláusulas.

Para dar respuestas a los objetivos planteados en este capítulo, nos servirán como instrumento de apoyo los diversos criterios u opiniones doctrinales, así como la jurisprudencia que aborda cuestiones relacionadas

(se suplanta para hacer pago con tarjeta o cuenta bancaria de la que no es el titular); b) suplantación del vendedor o servidor de pago (en este caso el estafador hace pasa por el vendedor para con el motivo de obtener los datos confidenciales sobre tarjeta o cuenta del cliente, con la intención de utilizarla en una compara fraudulenta. Esto se da en aquellos servidores web falsos que tiene la misma apariencia con comercio en la que el cliente quiere comprar; c) los datos almacenados en servidores poco segura (se da en aquellos casos en el que el cliente proporciona al vendedor sus datos y este lo almacena en su ordenador temporalmente para tramitar el pago con la entidad bancaria. Todo este riesgo se puede prevenir si los medios de pago electrónicos cumplen con ciertos requisitos por ejemplo: autenticación, confidencialidad, y no repudio", MARTÍNEZ GONZÁLEZ, M. "Mecanismo de…"*op., cit.,* pp. 6 y ss.

[511] MARIÑO LÓPEZ, A.: *Responsabilidad civil…op., cit.*, p. 410.

con la utilización fraudulenta[512] de tarjetas de pago en las operaciones llevadas a cabo en Internet. Además, han de tenerse en cuenta las disposiciones, comunitaria[513] y española[514], para el desarrollo de este capítulo.

En la doctrina española hay quien pone de manifiesto que "el fundamento de la responsabilidad de los prestadores de servicios de la sociedad de la información en los mecanismos de pago electrónico viene determinado por ausencia de presencia física de las partes en el mismo acto de cumplimiento y, por tanto la ausencia de control directo". Además "la

[512] El uso fraudulento o indebido de la tarjeta de crédito implica el uso no autorizado de la información de la tarjeta por parte de un tercero con el propósito de cargar gastos, en la cuenta del titular de la misma o extraer fondos de su cuenta. El fraude o el uso fraudulento de la tarjeta de crédito está considerado como una forma de robo de identidad. Es importante aclarar que basta con la numeración completa de la tarjeta, su fecha de caducidad y su CVV para poder realizar un uso fraudulento de la misma, sin necesidad de disponer físicamente de la misma.

[513] En el derecho comunitario tendremos en cuenta las siguientes disposiciones: la Recomendación de la Comisión 87/598/CE, de 8 de diciembre de 1987, sobre *«Código de buena conducta en materia de pago electrónico»* (relaciones entre organismos financieros, comerciantes-prestadores de servicios y consumidores); la Recomendación de la Comisión 88/590/CE, de 17 de noviembre de 1988, "relativa a los sistemas de pago y, en particular, a las relaciones entre titular y emisor de tarjetas"; la Recomendación de la Comisión 97/489/CE, de 30 de julio de 1997, "relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisor y titulares de tales instrumentos", en la que se establece la responsabilidad del emisor y del titular de la tarjeta ; y la Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007 "*sobre servicios de pago en el mercado interior"*, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE.(DOCE núm. L 43 de 14-2-1997).

[514] En el derecho español tendremos en cuenta las siguientes normativas: Ley 47/2002, de 19 de diciembre, de reforma de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista (LRLOCM), para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE, en materia de contratos a distancia, y para la adaptación de la ley a diversas directivas comunitarias, en *BOE*, núm. 304, de 20 de diciembre de 2002 ; Real Decreto-Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias; en especial el Libro segundo, Título II, Capítulo II (artículos 81 y siguientes) que regulan las condiciones generales de los contratos y las cláusulas abusivas[514]. Estos artículos sustituyen el art. 10, 10 bis y disposición adicional primera de la Ley 26/1984, de 19 de julio (LGDCU), en *BOE,* núm. 287 de 30 de noviembre de 2007; y la Ley 16/2009, de 13 de noviembre, de Servicios de Pago, que transpone al ordenamiento interno la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, de servicios de pago en el mercado interior. *BOE*., núm. 275, de 14 de noviembre de 2009).

ausencia de las partes en el acto determina que la entidad no controle la verdadera titularidad de la tarjeta, incluso aunque se establezca una clave privada, firma electrónica, por lo que el uso fraudulento de la misma o el error y la falta de control por parte de los prestadores de servicios de la sociedad de la información son circunstancias que determinan su responsabilidad[515]".

La suplantación de la identidad, el fallo del sistema, el uso fraudulento de los datos bancarios y el personal del titular de la tarjeta son las causas principales del conflicto existente entre las partes que intervienen en el sistema de pago electrónico. En el caso de que se produzcan dichos supuestos, hemos de plantear el siguiente interrogante: ¿quién debe asumir el riesgo por el uso fraudulento de la tarjeta o del número de la tarjeta en el comercio electrónico a través de Internet? Para resolver este interrogante centraremos nuestras posibles imputaciones de la responsabilidad civil a los siguientes sujetos: la entidad emisora/gestora de la tarjeta, el titular de la misma y los proveedores de bienes o servicios (establecimiento adherido al sistema), así como los entes intermediarios en el sistema de pago con tarjeta electrónica, por ejemplo, al proveedor de acceso a la red.

Antes de acometer el análisis de las distintas normativas sobre la responsabilidad de los sujetos intervinientes, es fundamental aclarar, que las Recomendaciones comunitarias que hemos venido mencionando a lo largo de este trabajo no son de carácter vinculante para las entidades bancarias. La que sí tiene carácter vinculante es la nueva Ley 16/2009, de 13 de noviembre, de servicios de pago.

[515] MORENO NAVARRETE, M.: *Derecho-e…op., cit.*, pp. 126 y ss.

4.1. La responsabilidad de la entidad emisora de la tarjeta de pago

4.1.1. Supuesto de responsabilidad de la entidad emisora

La entidad emisora y/o gestora de la tarjeta desempeña un rol fundamental en la prevención del uso indebido de la tarjeta[516] pues se encuentra sometida al cumplimiento de un conjunto de obligaciones básicas en virtud del contrato suscrito con el titular, así como en virtud del contrato firmado con el establecimiento adherido al sistema. El incumplimiento de estas obligaciones[517] por parte de la entidad emisora traerá como consecuencia la responsabilidad civil de la misma frente a los demás entes intervinientes en el sistema de tarjetas electrónicas de pago, por los daños ocasionados.

Según los criterios establecidos en las distintas normativas e instrumentos de autorregulación (la Ley 16/2009, de 13 de noviembre, de servicios de pago, Recomendaciones, Códigos de Conducta, y la Directiva 2007/CE), que hemos venido comentando a lo largo de esta investigación, la entidad emisora de la tarjeta será responsable frente al titular siempre y cuando nos encontremos en presencia de algunos de los siguientes supuestos[518]:

[516] MARIÑO LÓPEZ. A.: *Responsabilidad…op., cit.,*

[517] Transcribiendo textualmente las palabras de RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo…"*op., cit*., p. 320, quien sostiene que "los usos fraudulentos producidos, facilitados o provocados por el incumplimiento o un cumplimiento defectuoso de las obligaciones que incumben a la entidad emisora de la tarjeta son imputados a ésta (interceptación de los datos por quiebra de la seguridad del sistema informático de la pasarela de pago; duplicación de la banda magnética por instalación en un cajero de su red de una técnica de copiado; fuga de datos por la falta de medida de protección o actuación negligente de un empleado de la entidad…."; Criterio que compartimos.

[518] Véanse CARRASCOSA LÓPEZ, V; POZO ARRANZ, Mª. A y RODRÍGUEZ DE CASTRO, E. P. *La contratación…op., cit.,* p. 45; LAFUENTE SÁNCHEZ, R. *Los servicios financieros…op., cit.,* pp. 248 y ss; FERRANDO VILLALBA, Mª. De Lourdes. "El contrato de tarjeta de crédito", en ORDUÑA MORENO, Fco. J.; y TOMILLO URBINA, Jorge L. (dirs). *Contratación bancaria,* t II. Valencia: Tirant Lo Blanch, 2001, pp. 342-343.

- La no ejecución o ejecución incorrecta de las operaciones que impliquen el uso de la tarjeta, tanto por avería técnica o por cualquier otra anomalía atribuible al mismo[519]

- Las transacciones no autorizadas por el titular, siempre que el comprador niegue la transacción y no figure en ella su firma electrónica. Igualmente, en los supuestos de robo, extravío o pérdida de la tarjeta[520]

- Los fallos detectados en la cuenta del titular atribuibles a la gestión de la que es responsable la entidad emisora[521]

---

[519] Sobre este punto, las Condiciones Generales de Bankia, establecen en su cláusula noveno (9.1), que Bankia "responderá exclusivamente de las pérdidas directas que se pudieron ocasionar por la ejecución o ejecución incorrecta de operaciones debida al funcionamiento defectuoso de máquinas o sistemas situadas directamente bajo su control, limitando la responsabilidad hasta el importe de la operación. Además, dispone que la reclamación pertinente deberá efectuarse, salvo supuesto excepcional en el plazo máximo de dos días hábiles desde aquel en que tuvo lugar la operación fallida"; en esta misma línea, la clausulas 13 del Código de Buena Conducta**,** dispone que: « el emisor será responsable de las pérdidas directas en las que haya incurrido el tenedor de la tarjeta como consecuencia directa de un mal funcionamiento del sistema que está bajo su control. El segundo párrafo aclara que, el término «pérdidas directas» se refiere solamente al importe principal cargado en la cuenta del tenedor de la tarjeta, así como los intereses del mismo. El término «consecuencia directa» se refiere a todo el equipo e instalaciones en las que el emisor ha autorizado la utilización de la tarjeta»; sobre este mismo supuesto vid., el apartado primero del art. 75 de la Directiva 2007/64/CE*;* vid., SAP de Pontevedra (Sección 1ª), de 19 de septiembre de 2007, (*JUR*/50436).

[520] siguiendo la tesis mantenida por GUIMARÃES, quien señala que la entidad emisora de la tarjeta, "responde de las operaciones no autorizadas por el titular de la misma, aunque en última instancia puede repercutir esa responsabilidad en el comerciante beneficiario del pago, en la medida en que éste es quien prescinde de los elementos de legitimación del titular de la tarjeta, en cuanto acreedor de un servicio de pago electrónico, con vista a ampliar su mercado", GUIMARÃES, M. R.: "El pago mediante…"*op., cit.,* p. 201; LAFUENTE SÁNCHEZ, R. *Los servicios financieros…op., cit.,* p. 249; vid. SAP de Pontevedra (Sección 1.ª), de 19 de septiembre de 2007,(JUR/50436).

[521] Según se establece en el apartado 6.2 del anexo de la Recomendación de la Comisión 88/590/CE, «en cualquier controversia con el titular en relación con cualquiera de las operaciones a que se hace referencia en el primer, segundo y cuarto guión del punto 1 y en lo que respecta a la responsabilidad por una transferencia de fondos por medios electrónicos no autorizada, corresponderá al emisor probar que la operación fue correctamente registrada y correctamente contabilizada, y que no resultó afectada por alguna avería técnica o cualquier otra anomalía».

Respecto al primer supuesto, de la no ejecución o ejecución incorrecta de las operaciones que impliquen el uso del número de la tarjeta, tanto por avería técnica como por cualquier otra anomalía atribuible a la entidad emisora, el art. 45 de la Ley 16/2009, de servicios de pago, regula la responsabilidad de los proveedores de los servicios de pago (entidad emisora) en relación a dicho supuesto, y hace una diferenciación según las operaciones, ya sean las iniciadas por el ordenante (transferencias de crédito) o las iniciadas por el beneficiario (pagos con tarjetas)[522].

Según establece el párrafo primero, apartado primero de este mismo art. 45 de la LSP, «en el caso de las órdenes de pago iniciadas por el ordenante, su proveedor de servicios de pago será responsable frente a aquél de la correcta ejecución de la operación de pago hasta el momento en que su importe se abone en la cuenta del proveedor de servicios de pago del beneficiario. Producido este abono, el proveedor de servicios de pago del beneficiario será responsable frente al beneficiario de la correcta ejecución de la operación»[523].

[522] Vid. ALVARADO HERRERA, L. "La responsabilidad de los proveedores de servicios de pago en caso de no ejecución o ejecución defectuosa de operaciones en el proyecto de Ley de servicios de pago", en MADRID PARRA, A (dir.). *Derecho del sistema financiero y tecnología.* Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2010, p. 202; este autor comenta el art. 46 del proyecto de Ley de servicios de pago que actualmente fue sustituida por el art. 45 LSP.

[523] Sobre este punto, las Condiciones Generales de Bankia, establecen en su cláusula noveno (9.1), que Bankia "responderá exclusivamente de las pérdidas directas que se pudieron ocasionar por la ejecución o ejecución incorrecta de operaciones debida al funcionamiento defectuoso de máquinas o sistemas situadas directamente bajo su control, limitando la responsabilidad hasta el importe de la operación". Además, dispone que "la reclamación pertinente deberá efectuarse, salvo supuesto excepcional en el plazo máximo de dos días hables desde aquel en que tuvo lugar la operación fallida"; en esta misma línea, la clausulas 13 del Código de Buena Conducta**,** dispone que: « el emisor será responsable de las pérdidas directas en las que haya incurrido el tenedor de la tarjeta como consecuencia directa de un mal funcionamiento del sistema que está bajo su control. El segundo párrafo aclara que, el término «pérdidas directas» se refiere solamente al importe principal cargado en la cuenta del tenedor de la tarjeta, así como los intereses del mismo. El término «consecuencia directa» se refiere a todo el equipo e instalaciones en las que el emisor ha autorizado la utilización de la tarjeta»; sobre este mismo supuesto vid., el

Por otro lado, el párrafo segundo de este mismo precepto(art. 45) establece que, «en el caso de o peraciones de pago no ej ecutadas o ejecutadas defectuosamente, cuando el proveedor de servicios de pago del ordenante sea responsable con arreglo a lo dispuesto en el párrafo anterior, devolverá sin demora injustificada al ordenante la cantidad correspondiente a la operación y, en su caso, restablecerá el saldo de la cuenta de pago a la situación en que hubiera estado si no hubiera tenido lugar la operación de pago defectuosa».[524]

Al mismo tiempo, este artículo dispone en su párrafo tercero, apartado primero que «cuando el responsable con arreglo a lo dispuesto en el párrafo primero de este artículo sea el proveedor de s ervicios de pag o del beneficiario, éste pondrá inmediatamente a disposición del beneficiario la cantidad correspondiente a la operación de pago, abonando, en su caso, la cantidad correspondiente en la cuenta de aquel»[525].

Finalmente, el párrafo cuarto de este mismo art. 45 de la LSP dispone que «en todo caso, cuando una orden de pago procedente del ordenante no se ejecute o se ejecute defectuosamente, el proveedor de servicios de pago del ordenante tratará de averiguar inmediatamente, previa petición y con independencia de su responsabilidad con arreglo al presente apartado, los

---

apartado primero del art. 75 de la Directiva 2007/64/CE*;* vid. SAP de Pontevedra (Sección1.ª), de 19 de septiembre de 2007, (JUR/50436).

[524] En este mismo sentido, la directiva establece Cuando sea responsable el proveedor de servicios de pago del ordenante con arreglo a lo dispuesto en el párrafo primero, devolverá sin demora injustificada al ordenante la cantidad correspondiente a la operación de pago no ejecutada o ejecutada de forma defectuosa y, en su caso, restablecerá el saldo de la cuenta de pago a la situación en que hubiera estado si no hubiera tenido lugar la operación de pago defectuosa.

[525] Cuando sea responsable el proveedor de servicios de pago del beneficiario con arreglo a lo dispuesto en el párrafo primero, devolverá inmediatamente a disposición del ordenante la cantidad correspondiente a l a operación de pago y, en su caso, abonará la cantidad correspondiente en la cuenta de pago del beneficiario.

datos relativos a la operación de pago y notificará al ordenante los resultados»[526].

Por su parte, la Recomendación 88/590/CE dispone en su apartado 7.1 del anexo, que «sin perjuicio de lo dispuesto en los puntos 4 y 8, el emisor responderá frente al titular por la no ejecución o ejecución incorrecta de las operaciones del mismo a las que se hace referencia en el punto 1, incluso cuando la operación se inicie a través de mecanismos electrónicos que no estén bajo el control directo o exclusivo del emisor». El punto 7.2 del anexo de esta misma Recomendación 88/590/CE, se establece que «salvo lo dispuesto en el número 3 de este punto, la responsabilidad a que se refiere el número anterior tendrá la siguiente limitación: en caso de no ejecución o de ejecución incorrecta de una operación, la responsabilidad del emisor se limitará al importe de la operación no ejecutada o incorrectamente ejecutada».

[526] Según lo previsto en el apartado 2 del art. 45 de la LSP, «en el caso de órdenes de pago iniciadas por el beneficiario o a través de él, el proveedor de servicios de pago del beneficiario será responsable de la correcta transmisión de la orden de pago al proveedor de servicios de pago del ordenante. En estos casos, cuando la operación no se ejecute o se ejecute de manera defectuosa, por causa imputable a él, el proveedor de servicios de pago del beneficiario reiterará inmediatamente la orden de pago al proveedor de servicios de pago del ordenante.

Además, el proveedor de servicios de pago del beneficiario será responsable frente al beneficiario de la gestión de la operación de pago. En particular velará porque, una vez abonada en su cuenta la cantidad correspondiente a la operación de pago, tal cantidad esté a disposición del beneficiario inmediatamente después de producido dicho abono.

En el caso de órdenes de pago iniciadas por el beneficiario o a través de él, en las que, conforme a lo previsto en los dos párrafos anteriores, el proveedor de servicios de pago del beneficiario no sea responsable, la responsabilidad ante el ordenante por las operaciones de pago no ejecutadas o ejecutadas incorrectamente será del proveedor de servicios de pago del ordenante. En estos casos, el proveedor de servicios de pago del ordenante devolverá a éste, según proceda y sin demora injustificada, la cantidad correspondiente a la operación de pago no ejecutada o ejecutada de forma defectuosa y restablecerá el saldo de la cuenta de pago a la situación en que hubiera estado si la operación no hubiera tenido lugar".

En todo caso, cuando una orden de pago procedente del beneficiario no se ejecute o se ejecute defectuosamente, el proveedor de servicios de pago del beneficiario tratará de averiguar inmediatamente, previa petición y con independencia de su responsabilidad con arreglo al presente apartado, los datos relativos a la operación de pago y notificará al beneficiario los resultados».

Así mismo, la Recomendación 97/489/CE prevé en el inciso a) apartado 1 del art.8, que: «sin perjuicio de lo dispuesto en los artículos 5 y 6 en las letras a) y e) del apartado 2 del artículo 7, el emisor será responsable de la no ejecución o de la ejecución defectuosa de las transacciones del titular a que se refiere el apartado 1 del artículo 1, incluso cuando la transacción se inicie en un dispositivo o terminal o con un equipo que no esté bajo el control directo o exclusivo del emisor, siempre y cuando la transacción no se inicie en un dispositivo o terminal o con un equipo cuyo uso no haya autorizado este último»[527].

Sobre el segundo supuesto, cabe señalar que el art. 31 de la LSP, prevé que «sin perjuicio de lo dispuesto en el artículo 29 de la presente Ley, y de las indemnizaciones por daños y perjuicios a las que pudiera haber lugar conforme a la normativa aplicable al contrato celebrado entre el ordenante y su proveedor de servicios de pago, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada». Es decir, dicho precepto hace responsable al proveedor de servicios de pago (entidad emisora de la tarjeta) en el caso que éste realice operaciones de pago no autorizadas por el titular de la tarjeta.

En este mismo sentido, el apartado 7.1 del anexo de la Recomendación 88/590/CE, dispone, que el emisor responderá «de las operaciones no autorizadas por el titular». En esta misma dirección, el inciso b) del art. 8.1

[527] Vid. GÓMEZ MENDOZA, M. «Recomendación de la UE 97/489, de de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de tales instrumentos», en *RDBB*, núm. 69, enero-marzo 1998, pp. 252 y ss; PLAZA PENADÉS, J. contratación electrónica...*op., cit.,* p. 471.

de la Recomendación 97/489/CE dispone que el emisor de la tarjeta responderá «de las transacciones no autorizadas por el titular, así como de cualquier error o anomalía atribuible al emisor en relación con la gestión de la cuenta del titular»[528].

En el Código de Buena Conducta de la Banca Europea sobre los sistemas de pago mediante tarjetas, elaborado como respuesta a la Recomendación de la Comisión Europea relativa al sistema de pago, en su punto 11, se prevé que «el emisor deberá pagar la pérdida del importe resultante de una transacción no autorizada realizada con la tarjeta después de que el tenedor de la misma le haya notificado su pérdida, robo o copia, de acuerdo con los términos pertinentes»[529]; es decir, este punto hace responsable a la entidad emisora por el uso indebido de la tarjera, una vez que el tenedor o titular de la misma haya notificado la pérdida o sustracción de la misma.

A este respecto, el Servicio de Reclamaciones del Banco de España (SRBE) ha venido señalando reiteradamente que «después del aviso de pérdida, copia, robo o sustracción de la tarjeta dado por su titular, es la entidad la que ha de hacerse responsable de cualquier disposición que se haya podido llevar a cabo, pues, aunque demuestre que ha puesto todos los medios a su alcance para evitarlas, se estima que existe una

[528] Según se establece en el apartado 6.2 del anexo de la Recomendación de la Comisión 88/590/CE, «en cualquier controversia con el titular en relación con cualquiera de las operaciones a que se hace referencia en el primer, segundo y cuarto guión del punto 1 y en lo que respecta a la responsabilidad por una transferencia de fondos por medios electrónicos no autorizada, corresponderá al emisor probar que la operación fue correctamente registrada y correctamente contabilizada, y que no resultó afectada por alguna avería técnica o cualquier otra anomalía»

[529] Vid., el comentario de SÁNCHEZ-CALERO GUILARTE, J.: «Proyecto de Código bancario relacionado con los sistemas de pago electrónico», en *RDBB*, núm. 37, enero-marzo 1990, pp. 211 y ss.

responsabilidad objetiva en la entidad que es la que crea el sistema y lo implanta»[530].

El punto 6.1 de la Recomendación 88/590/CE prevé la carga de la prueba por parte del emisor, señalando «que en caso de controversia con el titular en relación con cualquiera de las operaciones a que se hace referencia en el primer, segundo y cuarto guión del punto 1 y en lo que respecta a la responsabilidad por una transferencia de fondos por medios electrónicos no autorizada, corresponderá al emisor probar que la operación fue correctamente registrada y correctamente contabilizada, y que no resultó afectada por alguna avería técnica o cualquier otra anomalía, sino que es atribuible a la responsabilidad del titular o usuario de la tarjeta, por el hecho de no haber conservado en lugar seguro su NIP o número secreto al violar su deber de secreto»[531].

Como se puede observar, las normativas a las que hemos hecho alusión a lo largo de este epígrafe hacen responsable al emisor cuando las operaciones se inicien a través de mecanismos electrónicos, aunque estos no estén bajo su control directo o exclusivo. A pesar de las responsabilidades establecidas por los preceptos mencionados con anterioridad, el punto 7.3 de la Recomendación 88/590/CE establece que

[530] Véanse las Memoria del SRBE correspondiente a los año 2005, p. 160; M 2007, p.191; y 2008; el SRBE, resuelve el siguiente caso: "(C A de Valencia, Castellón y Alicante (Bancaja), en el expediente n.º 1829/05, en la que señala que esta entidad bancaria se apartó de las buenas prácticas y usos bancarios al eludir su responsabilidad respecto del importe dispuesto con posterioridad a la comunicación del cliente, pues, si bien el bloqueo de la tarjeta por parte de la entidad no se llevó a cabo hasta un momento posterior a la ejecución de las disposiciones, el motivo de la demora entre la comunicación del cliente y la efectividad del citado bloqueo fue como consecuencia de los sistemas operativos que tiene establecidos la propia entidad, lo que en modo alguno resulta oponible ante su cliente), en Memoria del SRBE, (M 2005), p. 160.

[531] A juicio de GUIMARÃES, el "titular de la tarjeta no debe soportar la carga de la prueba del carácter fraudulento de operaciones, ni de la ausencia de la culpa por su parte, como sucede con los pagos realizados presencialmente, la carga de la prueba debe recaer sobre el emisor que, para recuperar la cantidad reclamada tendrá que demostrar que fue él el autor de las operaciones o que éstas se lo fueron posibles a causa de su negligencia". GUIMARÃES, M. R.: "El pago mediante…"*op., cit.,* p. 201,

«cualquier otra consecuencia financiera y, en particular, las cuestiones relativas al alcance del perjuicio por el que haya que pagar una compensación, se regirán por la ley aplicable al contrato celebrado entre el emisor y el titular»[532].

Hemos de citar como ejemplo algunas de las opiniones de los tribunales españoles en las que se hace responsable a la entidad emisora/gestora de la tarjeta por el uso fraudulento o indebido de la misma[533]. Según la tesis sostenida por la SAP de Málaga (Sección 4ª), de 7 de mayo de 2001, cuando no existe acuerdo entre las partes en un contrato de adhesión, «(...) el riesgo de fraude inherente al sistema, ha de ser asumido por la parte que se beneficia del sistema que no es otra que la entidad emisora del medio de pago, pues con respecto a ella el comerciante adherido tiene la condición de usuario, ya que paga por su utilización, y no la de socio, pues no participa en los beneficios de orden financiero que el sistema reporta a la entidad emisora, la cual, además, como consecuencia de la previsibilidad del riesgo, puede y en buena práctica comercial debe hacerlo, tener asegurado dicho riesgo, cargando el importe de la prima, en la parte correspondiente sobre la comisión que percibe del comerciante adherido por cada operación de venta por medio de la tarjeta».

---

[532] Vid. SÁNCHEZ GÓMEZ, A. *El sistema…op., cit.,* p.108; PLAZA PÉNADES, J. contratación…*op., cit*., p. 471. GÓMEZ MENDOZA, quien señala que no deja de haber una contradicción entre los puntos 7.2 y 7.3 de la Recomendación 88/590/CE, GÓMEZ MENDOZA, M. "Tarjeta…"*op., cit.,* pp. 397 y ss.

[533] Sobre la responsabilidad de la entidad emisora por la utilización de tarjeta por quienes no son sus titulares, el SRBE, en su Memoria correspondiente al año 2006, ha hecho alusión que "ni la doctrina ni la jurisprudencia mantienen una posición pacífica al respecto, ya que, si bien hay sentencias que sostienen que la entidad es una mera intermediaria, por lo que cualquier protesta por falsedad o demasía debe orientarse contra el institutor —sociedad que implantó el sistema— (Sentencia de la Audiencia Provincial de Madrid de 11 de abril de 1987), sin embargo, hay otras que mantienen lo contrario, ya que consideran que la única relación contractual del comercio es con el banco, es a este al que debe reclamar y obtener satisfacción, por cuanto fue el que efectivamente realizó el cargo en su cuenta (sentencias de 26 de octubre de 1998, de la Audiencia Provincial de Castellón, y de 13 de octubre de 2004, del Juzgado de Primera Instancia de San Sebastián"), en Memoria de Servicio del Reclamaciones del Banco de España, correspondiente al año 2006, p. 199, [En Línea] Disponible en Internet: http://www.bde.es (última consulta, 21 de abril de 2012).

Por su parte, la SAP de Baleares (Sección 3ª), de 28 de mayo de 2004[534] confirma la sentencia del Juzgado de Primera Instancia, en la que se declara la responsabilidad de la entidad emisora de la tarjeta de crédito sustraída y utilizada como medio de pago en diversos establecimientos comerciales con anterioridad a que su titular comunicara su sustracción.

La Audiencia Provincial de Sevilla (Sección 1. ª), en su sentencia de 31 de enero de 2005, resuelve un caso relacionado con la acción colectiva de cesación de condiciones generales de la contratación interpuesta por Ausbanc en defensa de los intereses colectivos de consumidores y usuarios. Según este tribunal, la entidad emisora de la tarjeta es responsable «(…) en caso de fallos del sistema, emisión de mensajes incorrectos que inducen a confusión e intervención fraudulenta por terceros, con la aplicación de la teoría del riesgo profesional inherente al tráfico bancario, sin desconocer la prevalente postura de la entidad por su posibilidad de acceso a datos y documentos con mayor facilidad probatoria, no siendo de recibo la exigencia de una prueba completa, por el titular de la tarjeta bancaria, por ser contraria a la equidad y entendiéndose que la exigencia de demostrar la coacción vulnera el justo equilibrio de las prestaciones y no guarda proporción y equidad».

En este mismo sentido, la Audiencia Provincial de Valencia (Sección 9. ª) en su sentencia de 17 de mayo de 2006[535] considera que el riesgo lo deben asumir las entidades emisoras.

Según la tesis sostenida por este tribunal «(…) las consecuencias perjudiciales que pueden derivar de tal riesgo en principio han de ser asumidas por las entidades bancarias pues son ellas la parte fuerte o dominante del contrato, las generadoras de la fuente del riesgo dado que

[534] JUR, 2004, 176397.
[535] AC/2006/1647.

son las que emiten las tarjetas e impulsan su uso en masa; las que marcan las reglas de funcionamiento y seguridad de la propia tarjeta fijadas en el propio contrato de adhesión y por último porque controlan y confeccionan los medios tecnológicos desplegados para su efectividad y su seguridad, pues son las que han configurado en el punto ahora que interesa, los cajeros automáticos, su ubicación y sus medidas de seguridad. Tal asunción de ese riesgo técnico determina la responsabilidad de las entidades bancarias tal como se reconoce por la mayoría de la Jurisprudencia (Sentencia de la Audiencia Provincial de Madrid, sección undécima 7-12-2002; Asturias 18-3-2002, y Tarragona, sección tercera, 27-12-2004, ésta última en un supuesto fáctico semejante al ahora enjuiciado) a no ser que el perjuicio causado sea imputable al titular de la tarjeta».

De todo lo expuesto a lo largo de este epígrafe llegamos a la conclusión de que la responsabilidad de la entidad emisora se quedará limitada al importe de la operación no ejecutada o defectuosamente ejecutada[536]; es decir, el emisor deberá resarcir al titular el importe de las transacciones no ejecutadas o incorrectamente ejecutadas y sus intereses. Y también, a la cantidad necesaria para permitir que el titular de la tarjeta recupere la situación que tenía antes de la realización de la operación no autorizada[537].

[536] Vid. GÓMEZ MENDOZA, M. "Recomendación de la UE 97/489,…*op., cit*.", p. 252.

[537] Según se establece en el párrafo segundo del punto 7.2 de la Recomendación 88/590/CE, «en el caso de una operación no autorizada, el importe de la responsabilidad será igual a la cantidad necesaria para permitir al titular recuperar la situación que tenía antes de realizar la operación no autorizada»; en este sentido, cabe mencionar el apartado primero del art. 60 de la Directiva 2007/64/CE**,** en la que se establece**,** que «Sin perjuicio del artículo 58, los Estados miembros velarán por que, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devuelva de inmediato el importe de la operación no autorizada y, en su caso, restablezca en la cuenta de pago en la cual se haya adeudado el importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada». Según pone de manifiesto LAFUENTE SÁNCHEZ, lo que se pretende en definitiva es resarcir al titular por los daños indirectos sufridos como consecuencia de la situación que le impidió disponer de sus saldos o realizar operaciones, LAFUENTE SÁNCHEZ, R. *Los servicios financieros…op., cit*., pp. 249 y 250; vid. GÓMEZ MENDOZA, M. "Recomendación de la UE 97/489,…*op., cit*.", p. 252.

El responsable de impedir el uso indebido de la tarjeta es el emisor quien a su vez debe responder por el mal funcionamiento del sistema ya que es quien conoce o debería conocer los riesgos y limitaciones de éste. Por lo que, la carga de la prueba recae en el emisor de la tarjeta. En este mismo sentido, algunos sectores que se dedican a velar por los intereses de los usuarios y consumidores, sostienen que la carga de la prueba se desplaza a la entidad emisora de las tarjetas, por ser ésta la que mayor facilidad probatoria tiene al disponer de los medios a su alcance para rastrear los movimientos realizados con las tarjetas[538].

Por último, se ha de hacer hincapié en que las recomendaciones comunitarias que hemos comentado no son vinculantes para las entidades bancarias, por lo que cabe resaltar que no garantizan los derechos de los consumidores frente al uso fraudulento del número de la tarjeta de crédito o débito en el comercio electrónico. Lo que sí es vinculante es la LSP.

4.2. Exención de responsabilidad

4.2.1. Cláusula de exención de responsabilidad por extravío o sustracción de la tarjeta de pago

En los contratos de emisión de tarjeta las entidades bancarias suelen incluir entre sus condiciones generales una cláusula de exoneración de responsabilidad por extravío, pérdida, robo o sustracción de la tarjeta o del NIP[539]. Es decir, existen condiciones generales del contrato de emisión que presentan en ocasiones disposiciones contractuales por las cuales la entidad

[538] Sobre la carga de la prueba véanse la Sentencia del Tribunal Supremo (Sala 1ª de lo civil), núm. 792/2009, de 16 de diciembre de 2009.

[539] MONTES RODRÍGUEZ, Mª. Pilar. "Las condiciones generales de los contratos bancarios y la protección de los consumidores y usuarios", en CUÑAT EDO, Vicente y BALLARÍN HERNÁNDEZ, Rafael (coords.). *Estudios sobre jurisprudencia bancaria.* Elcano (Navarra): Aranzadi, S.A., 2000, p. 108; PÉREZ RODRÍGUEZ, Ángela M. ª: "La responsabilidad por phishing en la banca electrónica. (Notas a propósito de la sentencia de primera instancia de Castellón de 25 de junio de 2008)", en MADRID PARRA, A (dir.). *Derecho del sistema financiero y tecnología.* Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2010, pp. 209-234.

emisora no asume responsabilidad alguna por la utilización indebida, antes de la notificación de la pérdida o sustracción de la tarjeta[540].

Pues bien, en este epígrafe abordaremos las cuestiones relacionadas con la validez de las cláusulas de exención o limitación de responsabilidad de la entidad emisora de la tarjeta, por extravío o sustracción de la misma antes de que su titular avise de su pérdida a la entidad emisora; y dejaremos para más adelante el análisis de las cláusulas abusivas. Ahora bien, el Código de Buena Conducta, en su cláusula 13 segundo párrafo, establece la exención de la responsabilidad de la entidad emisora señalando que ésta «no será considerada responsable por cualquier pérdida originada por una avería técnica del sistema de pago si dicha avería fuera reconocible para el tenedor de la tarjeta mediante un mensaje emitido en la pantalla del aparato, o fuera evidente de cualquier otra forma».

Al respecto, cabe destacar que existe una amplia y reiterada opinión jurisprudencial entorno a la exoneración de la responsabilidad de la entidad emisora de la tarjeta de crédito por el uso indebido. Así pues, citaremos por su claridad la SAP de Madrid (Sección 13ª), de 11 de mayo de 2005[541], al expresar que «si los hechos no se denuncian antes de transcurridas veinticuatro horas de su acaecimiento(…), cualquier cargo que se hiciese en la cuenta del cliente tras la sustracción o extravío de aquella es ajena a la responsabilidad de la entidad emisora de la misma en cuanto no se le haya comunicado por el interesado ni haya podido conocer por otro medio el hecho de su ilícita utilización».

[540] MARIÑO LÓPEZ. A.: *Responsabilidad civil…op., cit*., pp. 199 y ss; vid. NAVARRO CHINCHILLA, José Justo. "Condiciones generales y cláusulas abusivas en la contratación bancaria", en NIETO CAROL, Ubaldo (dir.). *Condiciones generales de la contratación y cláusulas abusivas.* Valladolid: Lex Novas, S.A., 2000, p. 547.

[541] (AC 2005, 832.); vid. SSAP de Madrid, de 5 de mayo 2005(JUR 2005,179031) y la de 25 de abril 2006(AC 2006, 873).

En este mismo sentido se pronuncia la SAP de Madrid (Sección 14ª), de 6 de febrero 2008, tras declarar la validez de la cláusula argumentando que cualquier cargo que se hiciese en la cuenta del cliente tras la sustracción o extravío de la tarjeta es ajena a la responsabilidad de la entidad emisora de la misma en cuanto no se le haya comunicado por el interesado ni haya podido conocer por otro medio el hecho de su ilícita utilización. De forma similar, han declarado la validez de la cláusula las sentencias de la Audiencia Provincial de Bilbao (sección 1ª), de 22 de septiembre de 2003, y (sección 5ª), de 28 de abril de 2005[542]; asimismo, la SAP de Castellón (Sección 1.ª), de 26 de octubre de 1998[543], sostiene que las cláusulas que obligan al titular de la tarjeta a comunicar de inmediato a la entidad emisora la sustracción o extravío de la misma, no son cláusulas abusivas, pero sí, en cambio, la que exonera totalmente de responsabilidad a la entidad emisora por los cargos realizados con tarjeta sustraída antes de tener el emisor conocimiento de dicha circunstancia.

Posición similar ha sostenido la SAP de Sevilla, de 4 de octubre de 2001 y la SAP de Asturias, de 31 de julio de 2001[544], con cita de las SSAP de Barcelona de 14 de septiembre de 1990, (Sección 12ª), de 14 de mayo de 1993[545] y de 4 de noviembre de 1997,que, examinando una cláusula similar, admitieron "la plena validez de la misma, sobre la base de que no exoneraba totalmente de responsabilidad a la entidad bancaria, sino sólo para el caso de sustracción de la tarjeta, y de que no se le podía imputar culpa a dicha entidad por la utilización fraudulenta de la misma".

[542] (AC 2005, 1406).
[543] (AC, 1998/213).
[544] PROV 2001, 311792.
[545] Según la SAP de Barcelona, 14 de 1993, "las clausulas establecidas no implica una exoneración de la responsabilidad del emisor, sino la libera de riesgo derivado de la pérdida o sustracción de la tarjeta que podría surgir del uso indebido del título crediticio para el titular del mismo, por la simples comunicación al centro emisor de dichas contingencias…."

También resulta de interés la Sentencia del Juzgado de Primera Instancia núm. 44 de Madrid, de 24 de septiembre de 2003, por cuanto declara la validez, en su Fundamento de Derecho Noveno, de la Cláusula «Séptima», en la cual se «prevé la exoneración de responsabilidad del Banco en aquellas operaciones que no interviene, como es la que se establece entre el cliente propietario de la tarjeta y el establecimiento ante el cual hace uso de la misma; lo contrario representaría obligar a quien no interviene en la relación a asumir sus consecuencias»[546]. En este mismo Fundamento de Derecho Noveno, el tribunal considera válida la cláusula «Octava», que «se refiere a la exoneración de responsabilidad del Banco por extravío o sustracción de la tarjeta de crédito (…) antes de la comunicación a la entidad».

Al mismo tiempo, señala la sentencia de referencia que si se admitiera la nulidad «lo contrario sería desplazar la obligación de custodia que tiene el propietario sobre dichos instrumentos», y a la vez aclara que «después de comunicar el extravío es el banco quien asume la responsabilidad que se derive de su actuación, no existe inversión de la carga de la prueba en caso de uso fraudulento del número secreto de la tarjeta; (…) si se produce es también consecuencia de la negligente custodia», y en la cláusula se incluye la exoneración de responsabilidad del titular cuando el uso de la tarjeta por tercero hubiere sido consecuencia de una coacción».

Ha de señalarse que ya existe jurisprudencia del Tribunal Supremo sobre lo relacionado con la notificación de la pérdida de la tarjeta. Así, la Sentencia del Tribunal Supremo (Sala 1ªde lo civil), de 16 de diciembre de 2009[547], que resuelve en recurso de casación una demanda presentada por la Organización de Consumidores y Usuarios contra la SAP de Madrid de 11 de mayo 2005, sostiene que, para que se consideren abusivas o nulas

[546] AC\2003\1475.
[547] (*RJ*\2010\702)

ciertas cláusulas, "la existencia de un extravío o sustracción debe comunicarse sin demora indebida desde que se conoció la desaparición".

Finalmente, resumiendo lo dicho a lo largo de este epígrafe, cabe señalar que, teniendo en cuenta las tesis sustentadas por las sentencias de los tribunales españoles que hemos comentado en relación con la validez de las cláusulas de exención de responsabilidad de la entidad emisora, por extravío o sustracción de la tarjeta, antes de que su titular notifique su pérdida, han de considerarse válidas dichas cláusulas, ya que se trata de cláusulas que exclusivamente exigen al titular de la tarjeta la obligación de notificar o comunicar con rapidez la sustracción, el extravío o pérdida de la tarjeta y su responsabilidad con anterioridad a la notificación[548].

4.3. Análisis del Real Decreto Legislativo 1/2007, de 16 de noviembre, de 2007, sobre cláusulas abusivas en relación con los contratos de tarjetas electrónicas de pago

En este epígrafe centraremos nuestro análisis en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU); en especial el Libro II, Título II, Capítulo II (arts. 82 a 90), que aborda las cuestiones relacionadas con las cláusulas abusivas. Dichos artículos sustituyen el art. 10, 10 bis y a la disposición adicional primera de la LGDCU, que examinan los requisitos legalmente establecidos que una cláusula debe contener para poder afirmar su carácter abusivo.

[548] MARIÑO LÓPEZ, A.: *Responsabilidad…op., cit*., p. 201; RECALDE CASTELLS, Andrés; PETIT LAVALL, María Victoria y JUAN Y MATEU, Fernando. "Cláusulas abusivas en los contratos bancarios", en MENÉNDEZ MENÉNDEZ, Aurelio y DÍEZ-PICAZO, Luis (dir). *Comentarios a la ley sobre condiciones generales de la contratación.* Madrid: Civitas, S.L., 2002, p. 1368.

Pues bien, antes de acometer dichas cuestiones, cabe señalar que el régimen de las cláusulas abusivas en la contratación electrónica será idéntico al de los otros tipos de contratos[549]. Por lo que, en la materia que nos ocupa (tarjeta electrónica), el régimen de las cláusulas abusivas que se aplicará será el Real Decreto Legislativo 1/2007, de 16 de noviembre (TRLGDCU).

4.3.1. Concepto de cláusulas abusivas

Antes de abordar las cuestiones relacionadas con las cláusulas abusivas, resulta necesario distinguir los dos conceptos esenciales: condiciones generales y cláusulas predispuestas, que terminológicamente se usan de manera indistinta. Las condiciones generales son las que han sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos[550]. En cambio las cláusulas predispuestas son aquellas cuya incorporación al contrato viene impuesta por una de las partes.

El art. 82.1 del TRLGDCU (sustituye el anterior art.10 bis de la LGDCU), da una definición de la «cláusula abusiva», que debe ser puesta en relación con los art. 85 a 90 del TRLGDCU, que contienen la lista que aparecía en la disposición adicional primera de la LGDCU en la que figura un catálogo especialmente ejemplificativo de cláusulas abusivas. Según prevé el

[549] GUISADO MORENO, Ángela. *Formación y perfección del contrato en Internet*. Prólogo de Leopoldo J. Porfirio Carpio. Madrid: Marcial Pons, Ediciones jurídicas y Sociales, S. A., 2004, p. 185 y ss; Vid. VEGA VEGA, A.: *Contratos…op., cit.,* p. 278.

[550] Vid. VILATA MENADAS, Salvador. "Condiciones generales de la contratación y el artículo 10 bis de la LGDCU", en *Protección de particulares frente a las malas prácticas bancarias II.* Publicación del Consejo General del Poder Judicial, núm. 79, 2006, pp. 52 y ss; vid. La Ley 7/1998 de 13 de abril, sobre condiciones generales de la contratación, define en su art.1 que "son condiciones generales de la contratación las cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes, con independencia de la autoría material de las mismas, de su apariencia externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos", en *BOE*, núm. 89, 14 de abril de 1998; vid. PARDO LÓPEZ, Javier. *Condiciones generales y cláusulas contractuales predispuestas. La Ley de condiciones generales de la contratación de 1998*. Prólogo de Juan Ignacio Font Galán. Madrid: Marcial Pons, Ediciones Jurídicas y Sociales, S.A., 1999, pp. 17 y ss.

apartado primero del art. 82 del TRLGDCU, se entiende por las cláusulas abusivas «todas aquellas estipulaciones no negociadas individualmente y todas aquéllas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe causen, en perjuicio del consumidor y usuario, un desequilibrio importante de los derechos y obligaciones de las partes que se derivan del contrato»[551].

Siguiendo lo planteado por el legislador español sobre el concepto de la cláusula abusiva, cabe señalar que, a nuestro juicio, las cláusulas abusivas no son más que aquellas condiciones impuestas en los contratos por las entidades emisoras de las tarjetas a los titulares o consumidores que perjudican sus derechos.

4.3.2. Requisitos para que una cláusula sea considerada abusiva

De la definición dada por el art. 82.1 del TRLGDCU, sobre las cláusulas abusivas, se desprenden los siguientes elementos o requisitos que son necesarios para que una cláusula pueda ser considerada abusiva:

[551] Véanse BLANCO PÉREZ-RUBIO, Lourdes. "Cláusulas abusivas en la contratación electrónica", en BOTANA GARCÍA, Gema (coord.). *Comercio electrónico y protección de los consumidores.* Madrid: La Ley, 2001, pp. 510 y ss; VEGA VEGA, A. *Contratos electrónicos…op., cit.,* p. 284; RIVERO ALEMÁN, S. *Crédito, Consumo…op., cit.,* p.171; PETIT LAVALL, Mª. V. *La protección del consumidor de crédito: las condiciones abusivas de crédito.* Valencia: Tirant Lo Blanch, 1996, p.130; vid. la Directiva 93/1993, del Consejo, de 5 de abril de 19 93, sobre las cláusulas abusivas en los contratos celebrados con consumidores, prevé en su apartado primero del art. 3 la definición de la cláusula abusiva considerando como tales aquellas «…cláusulas contractuales que no se hayan negociado individualmente se considerarán abusivas si, pese a las exigencias de la buena fe, causan en detrimento del consumidor un desequilibrio importante entre los derechos y obligaciones de las partes que se derivan del contrato» (*DOCE* núm. L 095 de 2 de abril de 1993 p. 29-34*)*; GONZÁLEZ PACANOWSKA, Isabel. "Condiciones generales y cláusulas abusivas", en BERCOVITZ RODRÍGUEZ-CANO, Rodrigo (dir.). *Comentario del texto refundido de la ley general para la defensa de los consumidores y usuarios y otras leyes complementarias. (Real Decreto Legislativo 1/2007).* Cizur Menor (Navarra): Aranzadi, SA, 2009, pp. 956 y ss; SERRA RODRÍGUEZ, Adela. *Cláusulas abusivas en la contratación. En especial, las cláusulas limitativas de responsabilidad*. 2. ª ed. Cizur menor (Navarra): Aranzadi, SA., 2002, p. 76; PARDO GATO, José Ricardo. *Las cláusulas abusivas en los contratos de adhesión (Análisis legislativo y jurisprudencial)*. Madrid: DIJUSA, S.L., 2004, pp. 87 y ss.

a. La existencia de un contrato en el que intervenga un consumidor[552].
b. La existencia de estipulaciones que no hayan sido negociadas individualmente y en cuyo contenido no haya podido influir el consumidor[553].
c. Que sean contrarias a la buena fe[554].
d. Que se produzca un desequilibrio importante de los derechos y obligaciones de las partes[555].

[552] Vid. BLANCO PÉREZ-RUBIO, L.: «El control de contenido en condiciones generales y en cláusulas contractuales predispuestas», en Separata de *Revista Jurídica del Notariado*, núm. 35 julio-septiembre 2000, pp. 22 y ss; VILATA MENATA, S. "Condiciones generales…"*op., cit.,* pp. 58 y ss.

[553] Sobre este requisito véanse el art. 3.2 de la Directiva 93/13/CEE, en la que se prevé que, "se considerará que una cláusula no se ha negociado individualmente cuando haya sido redactada previamente y el consumidor no haya podido influir sobre su contenido, en particular en el caso de los contratos de adhesión*";* vid. VEGA VEGA, A.: *Contratos…op., cit.,* pp. 279-281; BLANCO PÉREZ-RUBIO, L. «Las cláusulas abusivas en los contratos celebrados con consumidores: aplicación jurisprudencial de la Directiva 93/13», en *Separata de "Revista Jurídica del Notariado",* núm. 19 julio-septiembre 1996, pp. 206 -208.

[554] En relación con el requisito de la buena fe, el Considerando (16) de la Directiva 93/13/CE dispone que «en la apreciación de la buena fe hay que prestar especial atención a la fuerza de las respectivas posiciones de negociación de las partes, a si se ha inducido en algún modo al consumidor a dar su acuerdo a la cláusula y a si los bienes se han vendido o los servicios se han prestado a petición especial del consumidor; que los profesionales pueden cumplir la exigencia de buena fe tratando de manera leal y equitativa con la otra parte, cuyos intereses legítimos debe tener en cuenta»; vid. BLANCO PÉREZ-RUBIO, L.: "Cláusulas abusivas…"*op., cit.,* pp. 28 y ss; vid., GONZÁLEZ PACANOWSKA, I.: "Condiciones generales y...", *op., cit*., pp. 957 y ss; siguiéndonos el criterio establecido por DÍAZ-PICAZO, tras señalar que la buena fe es, "un arquetipo o modelo de conducta social: la lealtad en los tratos y el proceder honesto, esmerado y diligente; la fidelidad a la palabra dada; no defraudar la confianza que objetivamente se ha suscitado a los demás, ni abusar de ella, conducir conforme cabe esperar de quienes con honrado proceder intervienen en el trafico jurídico como contratantes o participes en él en virtud de otras relaciones jurídicas", en DÍAZ-PICAZO, L. *Fundamentos del Derecho Civil Patrimonial, vol. I: Introducción teórica del contrato*. Madrid: Civitas, 1996, pp. 50-51; ibídem, 398 p; VEGA VEGA, A.: *Contratos…op., cit.,* pp. 281 y ss.

[555] BLANCO PÉREZ-RUBIO, L.: "Cláusulas abusivas en…"*op., cit.*, pp. 527 y ss; Según pone de manifiesto la Confederación de Consumidores y Usuarios (CECU), en su informe de noviembre de 2007, sobre la cláusula abusiva en el comercio electrónico, que "como ejemplo ante este desequilibrio, encontramos cláusulas que, ante un incumplimiento por parte del consumidor, prevén la resolución del contrato de una manera rápida y fácil, frente a la que se prevé para el consumidor, más gravosa, en caso de incumplimiento de las obligaciones a cargo del vendedor. Otro caso es el supuesto de modificación unilateral que puede comunicarse por medio de página web y no directamente al consumidor y éste, que ante la modificación puede resolver el contrato, deba dirigirse en la forma y condiciones que

Según señala el legislador español, «el hecho de que ciertos elementos de una cláusula contractual o que una cláusula aislada se hayan negociado individualmente, no quiere decir que se excluya la aplicación de las normas sobre cláusulas abusivas al resto del contrato» (art. 82. 2 del TRLGDCU)[556]. Por lo tanto, el empresario que afirme que una determinada cláusula ha sido negociada individualmente, asumirá la carga de la prueba.

El párrafo tercero del art. 82 del TRLGDCU establece que, «el carácter abusivo de una cláusula se apreciará teniendo en cuenta la naturaleza de los bienes o servicios objeto del contrato y considerando todas las circunstancias concurrentes en el momento de su celebración, así como todas las demás cláusulas del contrato o de otro del que éste dependa»[557].

---

le especifican más gravosas para ejercer su derecho de resolución". [En línea] disponible en Internet: http://www.cecu.es(última consulta 20 de enero de 2012); vid., GONZÁLEZ PACANOWSKA, I. "Condiciones generales y..."*op., cit.,* pp. 960 y ss; para LASARTE ÁLVARES, "el desequilibrio en el contenido contractual al que alude el precepto sugiere, en efecto que el hecho de haber predispuesto unilateralmente el profesional el contenido del contrato tiene por objeto precisamente "abusar" de su posición de supremacía económica y de su capacidad de iniciativa contractual, de forma tal que sus obligaciones vengan aligeradas o disminuidas frente consumidor es colocado precisamente en la perspectiva contraria", en LASARTE ÁLVARES, Carlos. *Manual de protección de consumidores y usuarios.* Madrid: Dykinson, 2005, p.151; SERA RODRÍGUEZ, Adela. "Condiciones generales de la contratación y cláusulas abusivas en los contratos celebrados con consumidores", en REYES LÓPEZ, María José (coord.). *Derecho privado de consumo*. Valencia: Tiran Lo Blanch, 2005, pp. 340 y ss;

[556] En la doctrina FERNÁNDEZ PÉREZ, sostiene que " no parece que todas las previsiones del TRLGDCU resulten aplicables a estas cláusulas predispuestas de forma individual, porque no tiene excesivo sentido que una empresa establezca condiciones de este tipo, que desvirtúan los efectos de para el empresario de un clausulado general", en FERNÁNDEZ PÉREZ, N. *El nuevo régimen de la…*op., cit. p.129.

[557] Véanse GONZÁLEZ PACANOWSKA, I. "Condiciones generales y..."*op., cit.,* pp. 965 y ss; RIVERO ALEMÁN, S. *Crédito, Consumo…op., cit*., p.171; SERA RODRÍGUEZ, A. "Condiciones generales…" *op., cit.,* p.76; por su parte el art. 32. 2 de la PDDC, establece que "no obstante lo dispuesto en los artículos 34 y 38, el carácter abusivo de una cláusula contractual se apreciará teniendo en cuenta la naturaleza de los productos objeto del contrato y considerando, en el momento de celebración del mismo, todas las circunstancias que concurran en su celebración y todas las demás cláusulas del contrato, o de otro contrato del que dependa. Para evaluar la equidad de una cláusula contractual, la autoridad nacional competente tendrá también en cuenta la forma en que el comerciante ha redactado y comunicado el contrato al consumidor con arreglo al artículo 31"; vid., GONZÁLEZ PACANOWSKA, I. "Condiciones generales y..."*op., cit.,* pp. 965 y ss.

El apartado 4 del art. 82 TRLGDCU, dispone que «no obstante lo previsto en los apartados precedentes, en todo caso son abusivas las cláusulas que, conforme a lo dispuesto en los artículos 85 a 90, ambos inclusive: a) vinculen el contrato a la voluntad del empresario[558], b) limiten los derechos del consumidor y usuario[559], c) determinen la falta de reciprocidad en el contrato, d) impongan al consumidor y usuario garantías desproporcionadas o le impongan indebidamente la carga de la prueba[560], e) resulten desproporcionadas en relación con el perfeccionamiento y ejecución del contrato, o f) contravengan las reglas sobre competencia y derecho aplicable».

4.3.3. Nulidad de las cláusulas abusivas en el contrato de tarjeta electrónica de pago

El artículo 83 del TRLGDCU, que sustituye al apartado segundo del art.10 bis de la LGDCU, establece lo relativo a la nulidad de las cláusulas abusivas e integración del contrato. Según prevé este artículo: «las cláusulas abusivas serán nulas de pleno derecho, y se tendrán por no puestas» (83.1

[558] El art. 86 T RLGDCU establece que las cláusulas que determinen la exclusión o limitación de la obligación del empresario de respetar los acuerdos o compromisos adquiridos por sus mandatarios o representantes o supeditar sus compromisos al cumplimiento de determinadas formalidades.

[559] 1. La exclusión o limitación de forma inadecuada de los derechos legales del consumidor y usuario por incumplimiento total o parcial o cumplimiento defectuoso del empresario. En particular las cláusulas que modifiquen, en perjuicio del consumidor y usuario, las normas legales sobre conformidad con el contrato de los bienes o servicios puestos a su disposición o limiten el derecho del consumidor y usuario a la indemnización por los daños y perjuicios ocasionados por dicha falta de conformidad. *2.* La exclusión o limitación de la responsabilidad del empresario en el cumplimiento del contrato, por los daños o por la muerte o por las lesiones causadas al consumidor y usuario por una acción u omisión de aquél (art.86 del TRLGDCU.).

[560] Según establece el art. 88 TRLGDCU en sus apartados: 2. "La imposición de la carga de la prueba en perjuicio del consumidor y usuario en los casos en que debería corresponder a la otra parte contratante. 3. La imposición al consumidor de la carga de la prueba sobre el incumplimiento, total o parcial, del empresario proveedor a distancia de servicios financieros de las obligaciones impuestas por la normativa específica sobre la materia".

TRLGDCU). Según lo establecido en el precepto comentado diríamos que estamos ante una nulidad parcial del contrato[561].

Además, «la parte del contrato afectada por la nulidad se integrará con arreglo a lo dispuesto por el artículo 1.258 del Código Civil y al principio de buena fe objetiva» (art. 83.2 del TRLGDCU). Y, a continuación, señala el párrafo segundo de este mismo apartado segundo del art. 83 del TRLGDCU que «a estos efectos, el Juez que declare la nulidad de dichas cláusulas integrará el contrato y dispondrá de facultades moderadoras respecto de los derechos y obligaciones de las partes, cuando subsista el contrato, y de las consecuencias de su ineficacia en caso de perjuicio apreciable para el consumidor y usuario. Sólo cuando las cláusulas subsistentes determinen una situación no equitativa en la posición de las partes que no pueda ser subsanada podrá el Juez declarar la ineficacia del contrato»[562].

En relación con las cláusulas limitativas de responsabilidad, el párrafo segundo del art. 86 del TRLGDCU, que sustituye a la cláusula 10ª de la disposición adicional primera de la LGDUC, considera abusiva « la exclusión o limitación de la responsabilidad del empresario en el cumplimiento del

[561] Sobre este mismo argumento establecido en el precepto comentado vid., el art. 8.1 de la LCGC. Siguiendo el criterio mantenido por VEGA VEGA quien pone de manifiesto que se trata "de una nulidad parcial del contrato, puesto que las demás cláusulas quedaran subsistentes". Además señala, "que dicha nulidad viene incluso determinado por el art. 6.1 de la Directiva 93/13/CEE, tras establecer que los Estados miembros establecerán que no vinculan al consumidor, en las condiciones estipuladas por sus derechos nacionales, las cláusulas abusivas que figuren en un contrato celebrado entre éste y un profesional, y dispondrá que el contrato siga siendo obligatorio para las partes en los mismos términos, si éste puede subsistir sin las cláusulas abusivas", en VEGA VEGA, A.: *Contratos…op., cit.,* p. 286, nota nº 31; sobre este mismo pronunciamiento vid. SERA RODRÍGUEZ, A. "Condiciones generales…"*op., cit*., pp. 343 y ss; vid., GONZÁLEZ PACANOWSKA, I. "Condiciones generales y..."*op., cit.,* pp. 987 y ss.

[562] Véanse SANJUÁN y MUÑOS, Enrique. "Las condiciones generales de la contratación y el comercio electrónico", en *incorporación de las nuevas tecnologías en el comercio: aspectos legales,* Estudios de Derecho Judicial, núm. 71, CGPJ, Madrid, 2006, p. 32; VEGA VEGA, A.: *Contratos…op., cit.,* pp. 287 y ss; GONZÁLEZ PACANOWSKA, I. "Condiciones generales y..."*op., cit*., pp. 990 y ss; MARTÍNEZ ROSADO, J. « La Ley 44/2006, de…op., cit., pp. 148 y ss.

contrato, por los daños o por la muerte o por las lesiones causadas al consumidor y usuario por una acción u omisión de aquél».

A continuación, dedicaremos un epígrafe a analizar las diversas opiniones de los tribunales españoles, en los que estos abordan cuestiones relacionadas con las cláusulas abusivas en los contratos de tarjeta de crédito.

4.3.4. Incorporación de las cláusulas abusivas a los contratos de tarjeta de crédito

Se ha de señalar que las entidades emisoras de tarjetas de créditos para eximirse de responsabilidad en el caso de uso indebido o fraudulento de la tarjeta, incluyen cláusulas que podrían tener el carácter de abusivas en el contrato de tarjeta de crédito en los siguientes términos[563]:

[563] Asociación de Usuarios de Bancas y Seguros (ADICAE). *Ciclo de Seminarios Europeos contra el fraude en medios de pago. Retos y soluciones para los consumidores en medios de pago.* Zaragoza: Etita ADICAE, 2009, p. 97; Según señala ADICAE, la notificación "no es cuestión de tiempo, sino del momento preciso en el que se tiene constancia de la sustracción o extravío. Remitiéndose al Código Civil en su art. 1.255 dice que "los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público", disposición general que debe cumplir cualquier contrato lo que impide que existan cláusulas abusivas como la establecidas para el uso fraudulento con tarjetas"; por su parte la SAP de Madrid(Sección 21ª), de 18 de julio de 2007, resuelve un caso en el que la entidad bancaria establece cláusulas limitativas de responsabilidad. Según dispone *(…)* la cláusula 5ª sobre «Limitación de responsabilidad (...): el titular asume las responsabilidades derivadas de la utilización fraudulenta por terceras personas antes de la notificación prevista en el apartado b).3 de la cláusula 4ª. Esta responsabilidad queda limitada a un máximo de 25.000 Ptas. (150,25 €), siempre que la citada notificación se hubiera realizado antes de transcurridas las 24 horas del hecho que la motivó y siempre que no hubiera incurrido en dolo o negligencia grave. Sin perjuicio de otros supuestos, se entiende que concurre negligencia grave cuando la clave secreta está de tal modo unida a la tarjeta que el robo o extravío de ésta conlleva el conocimiento de la misma".

De acuerdo con la tesis mantenida por la SJPI, la Audiencia "procede confirmar la sentencia recurrida en cuanto a la declaración de nulidad del plazo de 24 horas que establece la cláusula 5ª del contrato de tarjeta de crédito, ya referido antes. Efectivamente dicha resolución parte de que no es contrario al equilibrio entre las posiciones de las partes la existencia de un reparto de responsabilidad entre ambas ni la limitación de responsabilidad contenida en la cláusula 5ª. Pero argumenta que sí rompe ese equilibrio el plazo tan breve establecido, de manera que se cumplirá sólo de forma excepcional,

- el titular de la tarjeta tiene un plazo de 24 horas para notificar la pérdida, robo sustracción o extravío[564]

- se limita a 150 euros la responsabilidad.

En este sentido, conviene señalar que existen opiniones de los tribunales españoles sobre la nulidad de las cláusulas insertas en las condiciones generales del contrato de tarjeta de crédito en virtud de las que se exonera a la entidad de responsabilidad por pérdida, sustracción, o robo de tarjeta de crédito. Al respecto, la Sentencia del Juzgado de Primera Instancia núm. 44 de Madrid, de 24 de septiembre de 2003, que hemos comentado con anterioridad en uno de los epígrafes de este capítulo, considera parcialmente la demanda de nulidad interpuesta por la Organización de Consumidores y Usuarios (OCU) ante el supuesto carácter

perjudicando de manera desproporcionada al consumidor. Valoración que comparte plenamente esta Sala y que es sustentada por la resolución que menciona la Juzgadora "a quo»; por su parte, la Sentencia de la Audiencia Provincial de Madrid(Sección 8ª), de 28 de noviembre de 2003, la cual añade que «el desequilibrio en los derechos del consumidor en lo atinente a la condición general que nos ocupa, no negociada individualmente, al haber sido redactada previamente y no haber podido aquél influir en su contenido, emerge desde el momento en que el tan manido plazo de veinticuatro (horas) dificulta enormemente la posibilidad de resarcimiento y comporta un correlativo beneficio para la demandada que se verá exenta de indemnizar más que en las ocasiones en que la notificación se realiza en ese exiguo "lapsus temporal", por lo que tiene carácter abusivo "por no atemperarse a las exigencias de la buena fe, ser desproporcionada, causar un notorio perjuicio al consumidor e implicar un desequilibrio claro en las obligaciones de las partes al respecto (...)».

[564] SAP de Madrid (Sección 8ª), de 28 de noviembre de 2003(PROV 2004, 89327). Según expresa este tribunal «que la condición general fijada en estas cláusulas, en relación con la utilización de las tarjetas, en cuanto hace mención al plazo de 24 horas, es abusiva y perjudica de manera desproporcionada al usuario que actúa de forma diligente denunciando sin demora, en cuanto tiene conocimiento de la sustracción o extravío, cuando en ese momento no puede ya hacer nada para evitar las sustracciones o disminuir la pérdida tanto si se han realizado en las 24 horas anteriores o en un plazo superior, y ello tras considerar: que está inserta en un contrato de adhesión, en el reverso del denominado contrato de tarjeta, en letra muy pequeña, sin estar especialmente resaltada y con la única referencia en el anverso a que se aceptan las condiciones impresas al dorso, sin suscripción independiente de las condiciones generales».

abusivo de c iertas cláusulas contenida en las condiciones generales del contrato de tarjeta de crédito.

Por su parte, la sentencia establece en su Fundamento de Derecho Octavo que es nula la cláusula «en la cual se exonera a la entidad bancaria de toda responsabilidad por fallos propios de su sistema informático o por la intromisión de terceros fuera del control del banco»; además añade que «ello supone desplazar la responsabilidad que incumbe al banco por el mal funcionamiento de s us servicios y organización administrativa hacia su cliente sin ninguna contraprestación para éste vulnerando el principio de responsabilidad por causación del daño cuando ninguna participación en él ha tenido el cliente perjudicado, lo cual implica una limitación de s us derechos contraria a lo dispuesto en la cláusula 14 de la repetida disposición adicional»[565].

Al mismo tiempo, este mismo Juzgado declaró la nulidad de aquellas cláusulas « (…) que declaran la exoneración del banco de toda responsabilidad por el mal funcionamiento de s u sistema operativo que afecte a la utilización de cajeros automáticos o terminales de capturas, sea cualquiera la causa, cuando el usuario o c liente no tiene ninguna intervención en los mismos».

En este mismo sentido, la Audiencia Provincial de Madrid (Sección 13ª) en su sentencia de 11 de mayo de 2005[566], resuelve el recurso de apelación planteado contra la ya citada SJPI núm. 44 de Madrid, de 24 septiembre de 2003. Así las cosas, según alega la parte demandante, en este caso la OCU, estos contratos contenían una cláusula según la cual «el banco no se responsabilizaba de los posibles daños o perjuicios que pudieran sufrir los clientes con motivo de i nterferencias, omisiones, interrupciones, virus

[565] *AC/* 2003/1475.
[566] AC/2005/832.

informáticos, averías telefónicas o desconexiones en el funcionamiento operativo del sistema elegido motivadas por causas ajenas al banco. De este modo, el banco tampoco se responsabilizaba de retrasos o bloqueos en el uso del sistema que fueran causados por deficiencias o sobrecargas de líneas telefónicas, en Internet, o en otros sistemas electrónicos, así como de los daños o perjuicios sufridos como consecuencia de errores, defectos u omisiones en la información facilitada por el banco, siempre que ésta procediera de terceros».

Finalmente, la Audiencia, apoyándose en la tesis sostenida por la sentencia del Juzgado de Primera Instancia, concluye que "la atribución de la responsabilidad hacia el cliente de la que corresponde en realidad soportar la entidad emisora es contraria a la cláusula 14 de la Disposición Adicional primera de la Ley General para la Defensa de los Consumidores y Usuarios, ya que este tipo de cláusulas suponen una limitación de los derechos del consumidor. De este modo, se trata de cláusulas ambiguas e indeterminadas y por tanto son nulas"[567].

[567] Sobre este mismo aspecto, siguiendo la tesis sostenida por ADICAE en uno de los trabajos o estudios publicado "estudio jurídico sobre el impacto del fraude", en la que "considera que las cláusulas que exonera a la entidad de toda responsabilidad en casos de interferencias, desconexión, avería en la red, son abusivas, desde el momento que la entidad declina toda responsabilidad incluido el caso que el problema venga ocasionado por los equipos del banco o por sus técnicos. No deben incluirse en este tipo de contratos una liberación absoluta de la responsabilidad de la entidad y hacer cargo con todos los perjuicios que se puedan ocasionar al consumidor. Al menos debería estipularse una carga de la prueba para la entidad, de que nada ha tenido que ver con la circunstancia acaecida". Por último, señala ADICAE que "una cláusula habitual en estos contratos es aquélla por la que la Entidad se exonera de toda responsabilidad por el uso fraudulento del sistema por parte de un tercero. Independientemente de la responsabilidad penal en la que pueda incurrir el tercero que se infiltra en el sistema, la Entidad no puede exonerarse de forma automática de toda responsabilidad, ya que en atención a lo establecido en la Ley de Protección de datos, puede tener una responsabilidad administrativa, desde el momento que permite el acceso a un tercero en su sistema. Además de la existencia de claves secretas, se hace necesario para operar a través de estos sistemas, la existencia de páginas seguras (https) por parte de la Entidad y la utilización de la Firma electrónica por el usuario a través de un ordenador seguro con sistemas antivirus". ADICAE. *Los fraudes en medios de pago…op., cit.,* p. 65.

Del mismo modo, la Sentencia del Tribunal Supremo (Sala 1.ª de lo civil), de 16 de diciembre de 2009[568], resuelve el recurso de casación que interpuso la Organización de Consumidores y Usuarios contra la mencionada sentencia de la Audiencia Provincial de Madrid (Sección 13ª) tras declarar la validez de varias cláusulas denunciadas. La Sala de lo Civil del Tribunal Supremo estimó parcialmente dicho recurso de nulidad. Entre las cláusulas que fueron anuladas por esta Sala, destacan especialmente las que hacían responsables a los titulares de tarjetas por el uso fraudulento o robo, en cuanto estas circunstancias no fueran comunicadas a las entidades emisoras.

Según afirma el alto tribunal, "las cláusulas que eximen de total responsabilidad a la entidad bancaria de manera indiscriminada y sin matización o modulación alguna son abusivas, como pone de relieve la OCU, porque contradicen la buena fe objetiva con desequilibrio en el sinalagma contractual en perjuicio del consumidor. Efectivamente, son advertibles situaciones en que, si la entidad actúa con la diligencia puede apercibirse de utilizaciones indebidas de tarjetas, aún sin la comunicación, o un eventual conocimiento de la sustracción o extravío. Son (…) frecuentes los casos en que la diligencia de las entidades advirtió utilizaciones indebidas, avisando incluso a los usuarios, que lo desconocían, del intento de utilización. Por ello, es desproporcionada una cláusula que se limite a la exoneración de responsabilidad, en todo caso, por el uso de la tarjeta antes de la notificación de la sustracción o extravío".

En este sentido, según califica la Sala 1ª de lo Civil del Tribunal Supremo, todas aquellas cláusulas en las que se obliga al titular a comunicar o notificar el extravío o sustracción de las tarjetas de crédito

[568] RJ\2010\702

"urgentemente"[569], "de forma inmediata"[570], "a la mayor brevedad"[571], de inmediato"[572], e incluso aquella que exige que "si los hechos no se denuncia antes de transcurridas 24 horas de su acaecimiento"[573], son abusivas, imprecisas e inciertas[574], por lo tanto, han de declararse nulas.

Además, considera desproporcionadas y abusivas todas aquellas cláusulas que exoneran de toda la responsabilidad a la entidad bancaria de las operaciones no autorizadas que se llevan a cabo antes de la notificación o aviso de manera indiscriminada, basando su fundamento en el art.23 y 32 de la LSP.

El art. 89.1 del TRLGDCU que sustituye a la cláusula 21. ª de la disposición adicional primera de la LGDUC, considera abusiva «la transmisión al consumidor y usuario de las consecuencias económicas de errores administrativos o de gestión que no le sean imputables». Según sostiene la doctrina, el carácter abusivo a que se refiere reside en que el predisponente desplaza sobre el consumidor riesgos[575]inherentes a su

[569]El vocablo utilizada por la entidad bancaria Bankinter, para exonerarse de la responsabilidad.

[570] La expresión empleada por BBVA.

[571] La terminología empleada por Santander Central Hispano (SCH).

[572] El Vocablo utilizada por SCH.

[573] Según señala el Supremo, no se declara abusiva la frase "antes de transcurridas 24 horas", sino el vocablo añadida por Caja Madrid, que es "de su acaecimiento", la que puede ser abusivo en caso en que no conoció la pérdida extravío, sin existir mala fe, ni falta de diligencia.

[574] Para DÍAZ RUIZ, "si bien no vemos la diferencia o mayor claridad de la fórmula que el Tribunal propone sobre las utilizadas por las entidades demandadas, salvo la de añadir "en cuanto si tenga conocimiento del hecho", pero que siempre que el usuario conozca que se ha perdido o le ha sido sustraída la tarjeta, si no la comunica de inmediato, cuando esto le sea posible, sin duda habrá demora indebida. Y en este sentido, la decisión del Tribunal Supremo no aclara, ni para los consumidores ni para las entidades de crédito gran cosa…", DÍAZ RUIZ Emilio. «Nulidad de las cláusulas abusivas en la contratación bancaria. (Comentario a la Sentencia de la Sala 1ª del Tribunal Supremo, núm. 792/2009, de 16 de diciembre de 2009)», en la *RDBB,* núm. 119, julio-septiembre 2009, pp. 279-306, en especial p. 300; vid. MARIMÓN DURÁ, R. *La tutela del usuario en el contrato bancario electrónico.* Monografía asociada a Revista Aranzadi de Derecho y Nuevas Tecnologías, núm. 8. Cizur Menor (Navarra): Aranzadi, S.A., 2010, p. 184 ver nota al pie 462.

[575] ANDREU MARTÍ. M. ª Del Mar. *La protección del cliente bancario.* Prólogo de José Miguel Embid Irujo. Madrid: Tecnos, 1998, p. 92.

actividad profesional que, por su calificación empresarial, debe sufrir.

Así, la Audiencia Provincial de Castellón (Sección 1. ª) en su sentencia de 26 de octubre de 1998[576] considera abusiva la cláusula que exonera de responsabilidad a la entidad emisora por los cargos realizados con tarjetas sustraídas antes de tener ésta conocimiento de lo sucedido; y la SAP de Asturias de 8 de mayo de 199 8[577], considera «(…) abusivas aquellas cláusulas que exoneran de responsabilidad en todo caso (es decir, sin tener en cuenta las circunstancias del caso concreto) a la entidad bancaria por los cargos realizados con tarjetas sustraídas antes de t ener el banco conocimiento de dicha circunstancia».

Lo mismo pone de manifiesto la Audiencia Provincial de Sevilla (Sección 6.ª) en su sentencia de 31 de enero de 2005[578] tras declarar la nulidad de dos cláusulas contenidas en las condiciones generales de un contrato de tarjeta del Banco Santander, en el que dicha entidad se exonera de responsabilidad por el uso fraudulento de la tarjeta, en caso de que el usuario no notifique su pérdida o sustracción y su uso indebido.

---

[576] *AC*/ 1998/ 2131.

[577] *AC*1998/1143.

[578] Se señala en la sentencia indicada que «…hay que recordar que la Ley 7/1998, de 13 de abril, cuyo ámbito son las condiciones generales de la contratación, tuvo por objeto la transposición de la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores, así como la regulación de las condiciones generales de la contratación, modificando el marco jurídico preexistente de protección al consumidor, constituido por la Ley 26/1984, de 1 9 de julio, General para la Defensa de los Consumidores y Usuarios, y que la acción que se ejercita encuentra su base en el artículo 8 de aquélla, que expresamente dispone que serán nulas de pleno derecho las condiciones generales que contradigan, en perjuicio del adherente, lo dispuesto en esta Ley y las que sean abusivas, cuando el contrato se haya celebrado con un consumidor, entendiendo por tales, en todo caso, las definidas en el art. 10 bis de la Ley 26/1984, de 19 de julio, General para la defensa de los Consumidores y Usuarios, y Disposición Adicional Primera de la citada Ley, precepto y Disposición que se introdujeron en esta Ley General por la Disposición Adicional Primera de la Ley 7/98 que la modificó, y en el art. 12 que establece y regula la acción colectiva de cesación para eliminar de dichas condiciones generales, en cuanto resulten contrarias a lo aquí dispuesto las que se consideren nulas con el pronunciamiento de condena al demandado tanto de su eliminación como de su utilización en lo sucesivo» (FD Primero).

En este mismo Fundamento de Derecho Primero, este tribunal sostiene que «la cuestión debatida se centra en los contratos de tarjeta de débito y crédito del Banco Santander Central Hispano, S.A. y en la condición, a modo de cláusula predispuesta, que viene a regular los supuestos de extravío o sustracción y su uso indebido condición novena de las condiciones generales del contrato de la tarjeta 4B Mastercard…».

Según establece dicha cláusula, «el titular y el tenedor de la tarjeta serán responsables, quedando el banco exento de toda responsabilidad por uso indebido, en los casos de carencia de notificación o defecto de ésta. En todo caso, el titular y el tenedor serán responsables si se demuestra que obraron de mala fe, dolo, culpa o negligencia e igualmente en todos los casos que se use el número secreto, salvo que se demuestre, en estos casos, que se vio obligado a revelarlo bajo coacción».

Además, la modificación citada de condiciones de tarjetas de débito y crédito establece que, "en los supuestos de extravío o sustracción de la tarjeta el límite de pérdida económica a cargo del contratante o, en su caso, del titular de la tarjeta, en caso de producirse se cifra en 150 euros hasta el momento de la notificación al Banco del hecho acaecido, salvo en operaciones que requieran marcaje del número secreto que serán en su totalidad a cargo del titular".

Considera la Audiencia que, en base a estas cláusulas, el banco emisor de la tarjeta “sólo respondería en caso de fallos del sistema, emisión de mensajes incorrectos que induzcan a confusión e intervención fraudulenta por terceros con la aplicación de la teoría del riesgo profesional inherente al tráfico bancario, sin desconocer la prevalente postura de la entidad por su posibilidad de acceso a datos y documentos con mayor facilidad probatoria, no siendo de recibo la exigencia de una prueba completa por el titular de la tarjeta por ser contraria a la equidad y entiende que la exigencia de

demostrar la coacción vulnera el justo equilibrio de las prestaciones y no guarda proporción y equidad".

También señala que son cláusulas predispuestas y redactadas unilateralmente por el banco del contrato tipo o de adhesión y discrepa en la interpretación de la sentencia apelada de que ninguna norma imperativa resulta infringida, en cuanto entiende que por el deber general de diligencia en el cumplimiento de las obligaciones de los artículos 1101 y 1104 del Código Civil "no debe aceptarse la exoneración total de responsabilidad del usuario de medios electrónicos de pago, por supuesta falta de seguridad del sistema y sí el derivado de una indebida custodia, con el beneficio para el consumidor del límite de su responsabilidad económica con el simple deber de comunicar a la Entidad la incidencia sufrida, con la genérica invocación de las disposiciones generales del Libro IV del Código Civil y el principio de libertad de pacto del artículo 1255".

Dichas cláusulas representan el traslado al titular de la tarjeta de todo riesgo por el uso indebido del medio de pago electrónico, lo que resulta abusivo y provoca un desequilibrio importante de derechos y obligaciones de ambas partes en perjuicio del consumidor y usuario.

Por lo tanto, este tribunal fundamenta su criterio resolutorio en lo siguiente: «que en definitiva, la cláusula, resulta contraria al requisito de equilibrio de los derechos y obligaciones de las partes y ocasiona, en principio del consumidor, un desequilibrio importante, al imponerse, en la práctica, una absoluta asunción de responsabilidad a cargo del titular de la tarjeta bancaria en los casos de utilización de la misma y de su número secreto, correlativamente supone una total exclusión de responsabilidad por parte del Banco, y por ello revistiendo el carácter de Abusiva, conforme a la Disposición Adicional Primera de la Ley 26/84 LGDCU, debe declararse su nulidad, así como la modificación que se opera a partir de uno de abril de

dos mil tres, entendiendo que la atenuación que se recoge y alega no es bastante, y que de la literalidad de referida cláusula o condición caben todos los supuestos, incluido el caso genérico de la pérdida de aquélla, pero es que las Recomendaciones de la Comisión Europea 88/590 CEE y 97/489/CEE contrastan con la asunción "en todo caso" por el titular de la tarjeta de la responsabilidad económica derivada de su uso fraudulento…».

Teniendo en cuenta lo planteado en el párrafo anterior, este tribunal condena a la entidad bancaria a eliminar dichos párrafos de la condición general novena de las condiciones generales de la contratación, u otros que en otros términos establezcan el mismo contenido de hacer responsable al titular de una tarjeta de débito o de crédito del uso indebido de la misma cuando se ha utilizado o marcado un número secreto u otro elemento de identificación similar.

Posición similar ha sostenido la SJPI núm. 2, de Castellón, de 25 de junio de 2008, en su Fundamento de Derecho Sexto, tras invocar la tesis sostenida por la SAP de Madrid (Sección 13ª), de 11 de febrero de 2005 (JUR 2005, 135114), en la que ésta señala, «que las referidas cláusulas desplazan la responsabilidad que incumbe al banco hacia su cliente que no ha tenido ninguna participación en el daño causado, infringiendo así lo contemplada en la cláusula 14 de la Disposición Adicional primera de la LGDCU(RCL 1984, 1906) en cuanto impone limitación de los derechos del consumidor»[579].

Al respecto añade la Instancia que, en efecto, no es dado imponer al consumidor la renuncia indiscriminada al derecho que le pueda asistir para reclamar, frente a la entidad que le proporciona los medios técnicos necesarios para una mejor o más cómoda prestación de sus servicios, en aquellos supuestos en los que, no mereciendo la consideración de caso

[579] *AC*/2008/1621.

fortuito o fuerza mayor así como los efectivamente no imputables a la propia entidad bancaria, le ocasionen daños y/o perjuicios. En este mismo sentido, se pronuncian entre otras la SAP de Zaragoza de 12 de abril de 2005; SAP de Madrid (Sección13ª), de 11 de febrero de 2005[580].

La Audiencia Provincial de Pontevedra (Sección 1ª), en la sentencia de 29 de julio de 2005[581] sostiene que «(…) la exoneración absoluta de responsabilidad que se recoge en el contrato debe reputarse nula y sin ningún efecto por entrañar una desproporción inadmisible en las obligaciones de las partes, puesto que, si bien la titularidad de una tarjeta de crédito comporta la obligación de custodiarla y, en caso de pérdida o sustracción, comunicar a la mayor brevedad lo sucedido, dicha obligación en absoluto puede relevar a la empresa adherida (comerciante), que obtiene mediante la tarjeta la seguridad del cobro de los servicios prestados, de utilizar la máxima diligencia para evitar adquisición de mercancías por quien no sea titular, (…)».

De este modo, añade el tribunal que «la cláusula de exoneración total de responsabilidad para el supuesto de utilización de la tarjeta por quien no es su titular durante el tiempo que medie hasta su notificación por correo certificado, se enmarca claramente en las cláusulas declaradas expresamente nulas por abusivas en el art. 10 bis de la Ley 26/84, de 19 de julio (RCL 1984, 1906), según redacción dada por la Ley 7/98 (RCL 1998, 960), de Condiciones Generales de la Contratación, y más concretamente, en los apartados 9º, que dentro del epígrafe II. Privación de derechos básicos del consumidor, sanciona con la nulidad toda cláusula que comporte la exclusión o limitación de forma inadecuada de los derechos legales del consumidor por incumplimiento total o parcial o cumplimiento defectuoso del profesional, y 15º, que con el rótulo «falta de reciprocidad», aplica la misma

[580] *PROV* 2005, 135114.
[581] *JUR*\2006\21845.

sanción a las cláusulas que entrañen «La imposición de obligaciones al consumidor para el cumplimiento de todos sus deberes y contraprestaciones, aún cuando el profesional no hubiere cumplido los suyos».

Según la tesis sostenida por la Audiencia Provincial de Valencia (Sección 9.ª), en su sentencia de 17 de mayo de 2006[582] «(…) hacer por vía contractual al consumidor responsable aun con limitaciones de cualquier supuesto de uso fraudulento de la tarjeta, resulta abusivo y contrario al principio del equilibrio de las prestaciones y por ende pacto nulo, concluyendo que ello determina la nulidad de pleno derecho de tal pacto».

A lo largo de este epígrafe hemos visto como las tesis sentadas por los tribunales españoles en relación con el carácter abusivo de las cláusulas de exoneración o limitación total de responsabilidad son uniformes. Se ha observado una línea constante de decisiones sobre la nulidad de las cláusulas insertas en las condiciones generales del contrato de tarjeta de crédito, siempre referido al cumplimiento de los requisitos establecidos en el art. 10 bis (sustituido por el art. 82 TRLGDCU).

4.4. Medidas adoptadas por las entidades bancarias para minimizar los riesgos y reducir la responsabilidad

En este epígrafe abordaremos las cuestiones relacionadas con las medidas adoptadas por la entidad emisora de la tarjeta con el fin de minimizar los riesgos y así reducir la responsabilidad. Según ponen de manifiesto las entidades emisoras de las tarjetas, las medidas de seguridad adoptadas para minimizar o evitar el riesgo y así reducir la responsabilidad son varias. Por ejemplo, los mecanismos de seguridad que incorporan las tarjetas, como el chip, el código NIP y el código de seguridad (CVV2 o

[582] Sentencia núm. 200/2006 de 17 mayo, Recurso de Apelación núm. 238/2006. (*AC*/2006/1647).

CVV)[583]que protegen a su titular de us os fraudulentos, reduciendo las consecuencias a que se exponen en caso de pérdida, robo, o extravío de la tarjeta[584].

En el capítulo II, epígrafe 2.2, de este mismo trabajo, se señala que para dotar de ni veles de seguridad a las transacciones electrónicas y a las operaciones comerciales, tales como la conclusión de contratos o el pago con tarjeta (de crédito o dé bito) realizadas en l nternet, es necesario el cumplimiento de un conjunto de el ementos básicos de s eguridad: la autenticación, integridad, confidencialidad y el no r epudio del origen y destino, que de forma preventiva, eviten usos fraudulentos de tarjetas en el comercio electrónico por un tercero no autorizado.

Además, se han de añadir los distintos protocolos de seguridad (SSL, SET y 3 D Secure)[585] de pago electrónico, así como la firma digital (que evita

[583] Los códigos CVV2 (visa) y CVC2 (MasterCard) son código de seguridad que aparecen en el reverso de cada tarjeta y contiene tres dígitos. Cabe destacar que éstos códigos presenta algunos inconvenientes para el titular de la tarjeta, en el caso de una sustracción o robo de la tarjeta, por un tercero, ya que éste último tendría en su poder la numeración e el códigos; en este mismo sentido, RICO CARILLO sostiene que es un mecanismo de seguridad implementado con la finalidad de facilitar la autenticación del titular del instrumento de pago en las operaciones a través de Internet. Se trata de un número compuesto por tres dígitos (…). Aun cuando este método contribuye a aportar seguridad a la operación de pago, sólo permite al proveedor asegurarse que la persona que está comprando tiene en su poder la tarjeta, el mecanismo no garantiza que sea el propio titular el que .está efectuando la operación, ya que al encontrarse el CCV impreso en el propio instrumento de pago, puede ser utilizado por cualquier persona que hay obtenido la tarjeta", en RICO CARRILLO, M. " La pr otección de l os consumidores en l as transacciones electrónicas de pago", en *Revista Electrónica de Estudio Télématique*, vol. 3, núm. 003, 2007, p.48, nota 4.

[584] Vid. HERNÁNDEZ GUARCH, Carlos. "Tarjetas", en LU NAS DÍAZ, María José (dir). *Malas prácticas bancarias.* Madrid: Formación AUSBANC, 2002, pp. 192 y ss; De hecho, en la doctrina RODRÍGUEZ DE LAS HERAS BALLELL quien advierte, que "corresponde a las entidades emisoras la adopción de una serie de medidas que impida el uso indebido de la tarjeta y minimicen sus consecuencias perjudiciales, entre estas medidas se encuentra la de informar y dar instrucciones al titular de la tarjeta sobre el uso y protección de la misma, del NIP y de los sistemas y cómo actuar en caso de extravío, robo, perdida o sustracción y; por otro lado dar instrucción al establecimiento adherido al sistema sobre los mecanismos de identificación del titular, el uso de los sistemas, la solicitud de autorización de la operación y el modo de actuar ante supuestos de uso indebido", en RODRÍGUEZ DE LAS HERAS BALLELL, T.: "El reparto de riesgo…"*op., cit.,* pp. 350 y ss.

que la transacción electrónica sea alterada por un tercero) y los certificados digitales (que es emitido por tercero, que garantiza la identidad de las partes), que las entidades emisoras de tarjetas utilizan para garantizar la seguridad a la hora de hacer compra por Internet.

Existen otras medidas que son imprescindibles para minimizar los riesgos, como, por ejemplo, la instalación de una versión actualizada de algún programa de antivirus y contar con un firewall. Al mismo tiempo, se recomienda hacer la compra en sitios web seguros y de confianza, por ejemplo direcciones que empiecen por (https//:) en cuya barra de navegador tiene que aparecer un icono de candado amarillo cerrado. Haciendo clic en el icono del candado aparecerá el nombre de la autoridad certificadora de la página.

4.5. Responsabilidad civil del titular de la tarjeta de pago por el uso fraudulento

4.5.1. Supuesto de responsabilidad del titular de la tarjeta ante el uso fraudulento en el comercio electrónico

Como señalamos con anterioridad en uno de los epígrafes del capítulo III, en virtud del contrato suscrito con la entidad emisora de la tarjeta, al titular de la misma le incumben varias obligaciones cuya finalidad es prevenir el uso fraudulento de la misma por personas ajenas o un tercero no autorizado. Por lo tanto, si el titular de la tarjeta incumple con dichas obligaciones, responderá en los siguientes supuestos:

- Por la demora en la notificación al emisor de la tarjeta de su pérdida, robo, extravío o sustracción

[585] Vid. MARTÍNEZ NADAL A. "Atribución de responsabilidad al comerciante o a la entidad bancaria proveedora del sistema de pago en caso de uso fraudulento de tarjetas en el comercio electrónico", en MADRID PARRA, A (dir.). *Derecho patrimonial y tecnología.* Prólogo de Manuel Olivencia. Madrid: Marcial Pons, 2007, p. 216.

- Por el uso negligente o doloso de la misma
- Por la utilización indebida o fraudulenta de la tarjeta de crédito
- Por la utilización indebida por parte de un tercero con el consentimiento del titular de la tarjeta

La doctrina considera que si se produjeran circunstancias que impliquen un riesgo de uso de la tarjeta por parte de terceros, ya sea por robo, pérdida, sustracción o extravío de la misma, el titular deberá comunicarlo a la entidad emisora/gestora de la tarjeta, ya que, de lo contrario, ésta última entendería que las operaciones llevadas a cabo en Internet, usando el número de la tarjeta o el NIP, habrían sido realizadas por aquel. De este modo, cuando concurra esta situación o s upuesto, de no c omunicar a la entidad emisora/gestora la pérdida o s ustracción de l a tarjeta, el titular será responsable de los gastos efectuados con la misma, en la tienda virtual (Internet) hasta el momento en que se notifiquen algunas de l as circunstancias mencionadas, siempre y cuando dicha notificación se produzca sin "excesiva demora" o "sin demora".

En cambio, la SAP de Madrid (Sección 11.ª) de 3 de octubre de 2006[586], resuelve un caso en el que expresa que el hecho de que la titular de l a tarjeta «…no comunicó a l a entidad emisora la sustracción antes del transcurso de las veinticuatro horas del acaecimiento que la apelante, ante la falta de otros datos(…) no significa que incurrió en dolo o negligencia grave, ni en ningún tipo de negligencia en la custodia de la misma, por lo tanto, la responsabilidad por las operaciones realizadas antes del aviso de l a sustracción de las tarjetas no debe asumirse por la actora en este caso, a pesar de no haber notificado a la demandada la sustracción antes del transcurso de las veinticuatro horas del acaecimiento de la misma, a la vista de las circunstancias concurrentes».

[586] *AC*\2007\715.

Según dispone el apartado primero del art. 32 LSP, «no obstante lo dispuesto en el artículo 31, el ordenante soportará, hasta un máximo de 150 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado o sustraído». Al mismo tiempo, el apartado 2 de este mismo art. 32 LSP establece que «el ordenante soportará el total de las pérdidas que afronte como consecuencia de operaciones de pago no autorizadas que sean fruto de su actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones con arreglo al artículo 27».

Asimismo, la Recomendación 88/590/CE, de 17 de noviembre de 1988, prevé, en el punto 8.3 del Anexo, que «el titular será responsable por la pérdida sufrida, hasta el momento de la notificación, por la pérdida, robo o falsificación del instrumento de pago, pero tan sólo hasta el equivalente de 150 ecus en cada caso, excepto cuando haya actuado con grave negligencia o fraudulentamente»[587].

Igualmente, la Recomendación 97/489/CE dispone en el apartado primero del art. 6, que «hasta el momento de la notificación, el titular asumirá los daños que resulten de la pérdida o del robo de su instrumento electrónico de pago hasta un determinado límite, que no excederá de 150 euros, excepto cuando haya actuado con negligencia grave, infringiendo lo dispuesto en la letras a), b) o c) del artículo 5[588], o de forma fraudulenta, en cuyo caso no se aplicará dicho límite»[589].

[587] Vid. FARRANDO MIGUEL, I. y CASTAÑER CODINA, Joaquín. «Atribución y distribución de responsabilidad civil por el uso no autorizado de tarjeta», en la *RDBB,* núm. 81, 2001, pp. 87-103, en p. 95, nota 28.

[588] Estos incisos se refieren a las diversas obligaciones que concierne el titular de la tarjeta. Pues bien, el inciso a) dispone, "que el titular utilizará el instrumento electrónico de pago en las condiciones aplicables a la emisión y utilización de tales instrumentos; en particular, tomará todas las medidas adecuadas para garantizar la seguridad del

Al respecto, debe tenerse en cuenta lo establecido por la Directiva 2007/64/CE[590] del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre "Servicios de pago en el mercado interior", por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE. Según dispone esta norma, en su apartado primero, art. 61, «no obstante lo dispuesto en el artículo 60, el ordenante soportará, hasta un máximo de 150 EUR, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado o robado o, si el ordenante no ha protegido los elementos de seguridad personalizados de la sustracción de un instrumento de pago»[591].

El apartado 2 del mismo art. 61, dispone que «el ordenante soportará todas las pérdidas que afronte como consecuencia de operaciones de pago no autorizadas y/o que sean fruto de su actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones con arreglo al artículo 56. En ese caso, no será de aplicación el importe máximo contemplado en el apartado 1 del presente artículo».

---

instrumento electrónico de pago y de los medios (número de identificación personal u otro código) que permitan su utilización"; b) "notificará sin demora al emisor (o a la entidad especificada por éste), en cuanto tenga conocimiento de ello: la pérdida o el robo del instrumento electrónico de pago o de los medios que permitan su utilización; el registro en su cuenta de cualquier transacción no autorizada; cualquier error u otra anomalía en la gestión de su cuenta por parte del emisor"; c) "no anotará su número de identificación personal u otro código de forma fácilmente reconocible, especialmente en el instrumento electrónico de pago o en cualquier objeto que guarde o que lleve junto con el mismo". Citado por, FARRANDO MIGUEL, I. y CASTAÑER CODINA, J. Atribución y distribución de...*op., cit*., p. 96, nota 35.

589 Vid., la SAP de Asturias (Sección 7ª), de 15 de febrero de 2005 *(AC* 2005, 422),

590 Unión Europea: publicado *DOUE*, L 319/27, 5 de diciembre del 2007.

591 En esta línea, el considerando (32) de la misma Directiva 2007/64/CE, establece que «a fin de ofrecer incentivos para que el usuario de servicios de pago comunique sin demora a su proveedor toda pérdida o robo de un instrumento de pago y reducir así el riesgo de operaciones de pago no autorizadas, el usuario solo debe ser responsable por un importe limitado, salvo en caso de fraude o grave negligencia por parte del usuario del servicio de pago.

Por su parte, el punto 12 del Código de Buena Conducta de la Banca Europea, determina que «el tenedor de la tarjeta pagará las pérdidas ocasionadas hasta el momento de la notificación al emisor de cualquier pérdida, robo o copia de la tarjeta. El tenedor pagará dichas pérdidas hasta un importe límite de 150 ecus, excepto cuando haya actuado de forma fraudulenta, a sabiendas, o haya cometido negligencia grave[592], o no haya cumplido con la cláusula 6 a), b) y c) del presente Código»[593]. Pues bien, este precepto hace responsable al titular de la tarjeta por el uso fraudulento de la misma antes de la notificación hasta un límite de 150 euros. Sin embargo, el precepto aclara que este límite no se aplicará si antes de la notificación el titular no ha cumplido con las obligaciones relacionadas con la custodia de la tarjeta y el NIP.

Conforme a lo establecido por el segundo párrafo de la cláusula 11 de la misma norma, «si el tenedor de la tarjeta hubiere actuado de forma fraudulenta, a sabiendas o por negligencia grave, pagará el total de lo perdido por transacciones no autorizadas realizadas después de la notificación, sin perjuicio de la obligación del emisor de entablar cualquier acción para evitar cualquier uso posterior de la tarjeta».

---

[592] SALAZAR BASCUÑANA, Lucio Martínez. *Condiciones generales y cláusulas abusivas en los contratos bancarios.* Cádiz: Editora de Publicaciones Científicas y Profesionales, S, L., 2002, p. 332.

[593] Según el criterio sostenido por el SRBE, en su Memoria de Reclamaciones correspondiente al año 2007, que los titulares de las tarjetas "son responsables de las disposiciones fraudulentas que hayan podido hacerse con sus tarjetas, mientras las entidades no hayan sido alertadas para que puedan bloquear las mismas. No obstante, en estos casos resultará de aplicación el límite de responsabilidad previsto en la norma 12 del ya aludido Código de Buena Conducta, por haberlo asumido voluntariamente las asociaciones profesionales del sector [que fija en 150 euros la cuantía máxima que por cargos fraudulentos debería asumir el titular, salvo que hubiese actuado de forma fraudulenta, a sabiendas o con negligencia grave, o no hubiera observado las cláusulas 6 (a) y (c) del Código, relativas a la necesidad de mantener la debida diligencia en la custodia de la tarjeta y su número secreto, así como a la obligación de comunicar su robo o extravío a la mayor brevedad posible]"; sobre este mismo aspecto, la (Memoria de Servicio de Reclamaciones, de 2008, p. 223), recoge este mismo criterio sostenido por la MSRBE de 2007), [En Línea] Disponible en Internet: http://www.bde.es.(última consulta 2 de diciembre de 2012); vid., SÁNCHEZ-CALERO GUILARTE, J.: "Proyecto de…"*op., cit.,* p. 214.

Tal como se prevé en la Ley 16/2007, de Servicios de Pago, y en las demás disposiciones comunitarias que hemos analizado a lo largo de este epígrafe, se ha de concluir que en los supuestos de uso fraudulento o indebido del número de la tarjeta, el titular será responsable hasta el momento de la notificación hasta un límite máximo exigible por las mencionadas normativas de 150 euros, siempre y cuando, aquel actúe de forma diligente[594], es decir, sin actuar de manera fraudulenta o con negligencia grave[595].

Por último, se ha de señalar que estaremos ante una conducta negligente por parte del titular de la tarjeta, cuando se efectúa el pago ilegítimo tras el conocimiento del número de la tarjeta, código de seguridad y otros datos personales del mismo como consecuencia de la suplantación, extravío o sustracción de la tarjeta, y el titular de la tarjeta no notifica a la entidad emisora tales hechos, por lo que dicha actitud negligente le haría

[594] Según sostiene el Banco de España, en su resolución de la reclamación de 1991, no son ajustado a las buenas prácticas bancarias no aplicar al titular de la tarjeta el límite de responsabilidad referido (véanse los informes relativos a las reclamaciones 1334/91, 14/91 y 25/92).

[595] De hecho, suscribiendo el criterio sostenido por los autores FARRANDO MIGUEL, y CASTAÑER CODINA, quienes han señalado que, "el retraso o la comunicación de la pérdida, sustracción o robo de la tarjeta puede llegarse a considerarse una conducta negligente, pero sobre la misma no cabe establecer una regla general ya que si bien es posible encontrar decisiones que consideran que el retraso de 38 días en comunicar a la entidad emisora la sustracción, "no se considera de la suficiente entidad para generar responsabilidad en el titular" [SAP de Baleares (Sección 5.ª), de 26 de febrero de 1997(Actualidad Civil (AC), 1997-3 21115)], otras consideran diligente la comunicación efectuada "el primer día hábil siguiente a aquel en que se verificó la sustracción" SAP de Bilbao de 19 de diciembre de 1986 (La Ley 1987-2, 252 p.), sin embargo, en otras se ha apreciado la negligencia al haber trascurrido un mes y 12 días desde la sustracción (SAP de Barcelona (Sección 12ª), de 14 de mayo de 1993 (La ley 1993-2, 451p.), 44 días (SAP de Barcelona (Sección 16ª), de 14 de septiembre de 1990 (558 Revista General de Derecho (RGD), 1991, 1811p.), más de tres meses (SAP de Málaga (Sección 4ª), de 9 de septiembre de 1994 AC, 1995-1, 387), más de 10 días SAP de Barcelona (Sección 17ª), de 4 de noviembre de 1997(646/647 (RGD) 1998, 10088 p), 5 días desde su extravío o sustracción(SAP de Barcelona(Sección 17.ª), de 25 de enero de 1999(*RJC* 1999, 417)], FARRANDO MIGUEL, I. y CASTAÑER CODINA, J. «Atribución y distribución…»*op., cit.,* p. 98, nota 43; sobre este mismo aspecto véanse BUSTO LAGO, José Manuel (coord). *Reclamación de consumo. Derecho de consumo desde la perspectiva del consumidor*. Elcano (Navarra): Aranzadi, 2005, pp. 734 y ss.

responsable de los daños ocasionados[596]. Es decir, el titular asume la responsabilidad de la custodia de la clave privada y por ello, las consecuencias de una conducta negligente en su conservación[597].

4.5.2. Las cláusulas de exención de la responsabilidad del titular de la tarjeta electrónica

Sobre la exoneración de la responsabilidad del titular por el uso fraudulento de la tarjeta de crédito o NIP, hemos de tener en cuenta lo establecido en las distintas normativas que hemos comentado con anterioridad. Asimismo, el legislador español establece en el apartado 3 del art. 32 LSP, que «salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 27.b, de un instrumento de pago extraviado o sustraído». Al mismo tiempo, el apartado 4 de este mismo art. 32 LSP, dispone que «si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 28.1.c, el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta».

Según dispone la Recomendación 88/490/CE, en su punto 8.2 del anexo, «una vez que el titular haya notificado la pérdida a la agencia central, con arreglo a lo dispuesto en la letra b) del número 1 del punto 4, quedará exento de responsabilidad; no obstante, la presente disposición hace hincapié que

[596] Vid. CASELLAS, David. "obligaciones y responsabilidad excesiva para los usuarios", en *Ciclo de seminarios europeos contra el fraude en medios de pago. Retos y soluciones para los consumidores en el fraude en medios de pago.* Zaragoza: ADICAE, 2009, p. 46.
[597] RIBAS ALEJANDRO, J. *Riesgos legales en Internet…op., cit.,* p. 149.

no será de aplicación cuando el titular haya actuado con grave negligencia o fraudulentamente».

En este sentido, el apartado segundo del art. 6 de la Recomendación 97/489/CE establece que «a partir del momento en que el titular haya notificado al emisor (o a la entidad especificada por éste) la pérdida o el robo de su instrumento electrónico de pago, de conformidad con lo dispuesto en la letra b) del artículo 5, no será responsable de los daños que resulten de los mismos excepto cuando haya actuado de forma fraudulenta»[598].

Al mismo tiempo, hay que tener en cuenta lo establecido en el apartado tercero del mismo art.6.3 que exime de responsabilidad al titular tras establecer que «no obstante lo dispuesto en los apartados 1 y 2, el titular no será responsable si el instrumento de pago se utilizó sin presentación física o identificación por medios electrónicos del instrumento mismo. El uso exclusivo de un código confidencial o cualquier otro elemento similar de identificación no será suficiente para entrañar su responsabilidad»[599].

[598] Sobre este aspecto comenta MARTÍNEZ NADAL, cuando se dan estas circunstancias "seria las reglas generales de responsabilidad en caso de usos indebidos con pérdida o sustracción de la tarjeta, aceptadas también por la doctrina y jurisprudencialmente, y en virtud de las cuales responde de forma objetiva el titular hasta el momento de la notificación, en que se traslada la responsabilidad a la entidad emisora", MARTÍNEZ NADAL, A. «El pago con tarjeta en la contratación electrónica. En especial, el art. 46 LOCM», en *RDBB*, núm. 84, octubre-diciembre 2001, p. 68.

[599] Siguiendo el criterio sostenido por FRAMIÑAN SANTAS, quien señala que "en el caso de la tarjeta que puede ser utilizada el sistema SET en la red no existe presencia física de la misma ni tampoco identificación electrónica del sistema mismo". El sistema SET descansa (…) fundamentalmente en un sistema de certificado de claves públicas y privadas que únicamente garantizan que una determinada persona posee una tarjeta y una clave pública determinada –que se debe corresponder con una determinada clave privada--. Pero no impide que un tercero ajeno a titular llegue a utilizar la tarjeta utilizando las claves privadas del titular, situación que el empresario o proveedor no puede detectar (…). Añade este autor, que a pesar de que el titular le incumbe una serie de obligaciones de custodia, de notificación y utilización del programa en la forma determinada por la entidad emisora el incumplimiento de la misma que acabe en un uso ilegítimo de la tarjeta en la red, la entidad emisora vendrá obligada a restituir las cantidades de las que se dispuso en virtud de la orden irregular. Y que dicha entidad no podrá ni siquiera librarse de su responsabilidad demostrando que el uso irregular de la tarjeta se debió a una negligencia del titular de la tarjeta". FRAMIÑAN SANTAS, J. "Pagos en la…"*op., cit*., p. 384; vid. AZOFRA VEGAS,

Conforme a lo dispuesto en el art. 61.4 de la Directiva 2007/64/CE, «salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 56, apartado 1, letra b), de un instrumento de pago extraviado, robado o sustraído»[600]. De este modo, el apartado 5 de este mismo art. 61 dispone que «si el proveedor de servicios de pago no ofrece medios adecuados para que pueda notificarse en todo momento el extravío, el robo o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 57, apartado 1), letra c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta».

Por su parte, SRBE establece en sus Memorias de Reclamaciones del 2007 y 2008, que « después del aviso de pérdida, copia, robo o sustracción de la tarjeta dado por su titular, es la entidad la que ha de hacerse responsable de cualquier disposición que se haya podido llevar a cabo, pues, aunque demuestre que ha puesto todos los medios a su alcance para

Fernando. «La contratación electrónica bancaria», en *RDBB*, núm. 68, octubre-diciembre 1997, pp. 1109-1119, en especial p. 1111; PLAZA PENADÉS, J.: "Contratación…"*op., cit.,* p. 471.

[600] Según prevé el apartado 3 del art.61.de la Directiva 2007/64/CE "en aquellos casos en que el ordenante no haya actuado de forma fraudulenta ni haya incumplido de forma deliberada sus obligaciones con arreglo al artículo 56, los Estados miembros podrán reducir la responsabilidad establecida en los apartados 1 y 2 del presente artículo, teniendo especialmente en cuenta la naturaleza de los elementos de seguridad personalizados del instrumento de pago y las circunstancias de la pérdida, el robo o la sustracción"; El considerando (32) de la misma Directiva 2007/64/CE dispone que, «(…), una vez que el usuario haya comunicado al proveedor de servicios de pago que su instrumento de pago puede haber sido objeto de uso fraudulento, no deben exigírsele responsabilidades por las ulteriores pérdidas que pueda ocasionar el uso no autorizado del instrumento. La presente Directiva se entiende sin perjuicio de la responsabilidad de los proveedores de servicios de pago por la seguridad técnica de sus propios productos».

evitarlas, se estima que asume esa responsabilidad al crear el sistema e implantarlo...»[601].

Sobre la exención o exoneración de la responsabilidad del titular de la tarjeta ya ha tenido ocasión de pronunciarse la jurisprudencia española. Así, la Audiencia Provincial de Madrid (Sección 14ª) en su sentencia de 25 de abril de 2006, afirma que «la responsabilidad por las operaciones realizadas antes del aviso de la sustracción de las tarjetas no debe ser asumido por el titular de la misma, a pesar de no haber notificado a la entidad emisora de la tarjeta la sustracción antes del transcurso de las veinticuatro horas del acaecimiento de la misma, a la vista de las circunstancias concurrentes,…». En este mismo sentido pronuncia, la Sentencia de la Audiencia Provincial de Asturias (Sección 5ª), de 18 de marzo de 2002[602].

La Audiencia Provincial de Tarragona(Sección 3ª) en su sentencia de 27 de diciembre de 2004 sostiene que "en consecuencia, caso de constatarse las disposiciones no autorizadas por tercero y obtenidas de forma ilícita, sólo el titular de la tarjeta será responsable en caso de un uso negligente o falta del deber de diligencia en las obligaciones de custodia y secreto, pues fuera de tales casos el riesgo técnico tendrá que ser asumido por la parte fuerte contratante y que impulsa el sistema (criterio igualmente fijado en la sentencia de Audiencia Provincial de Murcia-sección primera-29/9/2004)". Sobre este mismo aspecto, la Audiencia Provincial de Valencia (Sección 9ª) en su sentencia de 17 de mayo de 2006, siguiendo el criterio también fijado por la SAP de Murcia de 29 septiembre 2004, establece que, «el titular de la tarjeta solo será responsable en caso de un uso negligente o falta del deber de diligencia en las obligaciones de custodia y secreto, pues fuera de tales casos el riesgo técnico tendrá que ser asumido por la parte fuerte

[601] Vid., Memoria SRBE correspondiente al año 2 007, p.191; vid., la Memoria SRBE correspondiente al año 2008; Memoria SRBE correspondiente al año 2006; Memoria SRBE correspondiente al año 2005.

[602] (*AC*/2002/604).

contratante y que impulsa el sistema».

Tras analizar las diversas opiniones sostenidas por los tribunales españoles a lo largo de este epígrafe, las conclusiones a las que llegamos son las siguientes:

Que se ha de destacar que existe una gran disconformidad de opiniones a la hora de calificar un determinado comportamiento del titular de la tarjeta como negligente[603]que es el elemento determinante de que se le pueda imputar responsabilidad.

Y que, por último, cabe reseñar que el titular de la tarjeta sólo quedará exonerado de las responsabilidades que se le atribuyen, una vez que notifique la sustracción, pérdida, robo o extravío de la tarjeta.

4.6. Responsabilidad del proveedor de bienes o servicios

Según las consideraciones expuestas en uno de los epígrafes del capítulo III, al proveedor de bienes o servicios le corresponden una serie de obligaciones relacionadas con el pago con tarjeta, ya sea presencial o no. Así pues, el objetivo de este epígrafe se limita a examinar las posibles imputaciones de responsabilidad al proveedor de bienes o servicios cuando existe cargo fraudulento o indebido mediante el uso del número de una tarjeta de pago en el comercio electrónico a través de Internet.

A continuación analizaremos aquellos supuestos en los que se puede atribuir el riesgo y la posible responsabilidad del proveedor de bienes o servicios en el caso del uso fraudulento o indebido mediante el uso del número de la tarjeta de pago en la operativa de pago electrónico.

[603] Vid. BUSTO LAGO, J. M (coord.). *Reclamaciones de consumo…op., cit.,* p. 743.

4.6.1. El cargo indebido o fraudulento mediante el uso de la tarjeta de pago en el comercio electrónico a través de internet

En los últimos años, el legislador español aprobó algunas normativas que de una forma u otra regulan cuestiones relacionadas con el pago mediante tarjeta en la contratación a distancia. Por ejemplo, la Ley 47/2002, de 19 de diciembre (LRLOCM) que modifica en su art. 3 al art. 46 de la Ley de Ordenación del Comercio Minorista (LOCM), dedicado al «pago mediante tarjeta». Antes de efectuarse dicha reforma, este precepto establecía que «cuando el importe de una compra hubiese sido cargado utilizando el número de una tarjeta de crédito, sin que esta hubiese sido presentada directamente o identificada electrónicamente, su titular podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular se efectuarán a la mayor brevedad».

Sin embargo, la nueva redacción dada por el precepto tercero de la LRLOCM prevé lo siguiente: «cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, su titular podrá exigir la inmediata anulación del cargo». Y concluye que, «en tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular se efectuarán a la mayor brevedad»[604].

[604] Según señala la Memoria de Servicio de Reclamaciones de Banco de España de 2008, que con la reforma de la LOCM, el legislador español introduce un cambio en la redacción del precepto 46.1 LOCM, según lo previsto en el artículo tercero de la Ley 47/2002, de 19 de diciembre (LRLOCM); y que "la nueva redacción de este precepto pretende transmitir a los usuarios de este medio de pago la seguridad de que su uso fraudulento está protegido jurídica y comercialmente con la retrocesión del cargo efectuado, siempre y cuando no exista constancia documental del titular de la tarjeta y este excepción la compra realizada. Ello no obstante, exige que el uso de esta tarjeta haya sido fraudulento o indebido, ya que lo contrario supondría la posibilidad de excepcional cualquier compra por el mero hecho de que la misma se hubiera realizado utilizando el número de una tarjeta de pago, pues esa prerrogativa supondría colocar en una posición de inseguridad jurídica al comerciante de

En este mismo sentido, el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, en su capítulo IV, art. 106 regula el pago mediante tarjeta. Así pues, según prevé el apartado primero de este mismo precepto 106 TRLGDCU, «cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, el consumidor y usuario titular de ella podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del empresario y del consumidor y usuario titular de la tarjeta se efectuarán a la mayor brevedad».

En relación al precepto que hemos comentado en el párrafo anterior (art. 106 del TRLGDCU), se ha de señalar que dicho artículo reproduce literalmente lo establecido por el art. 46 LOCM, tras su reforma por la LRLOCM. No obstante, se introdujeron algunas modificaciones, que no afectan a LR LOCM, ya que sólo se trata de la sustitución de algunas expresiones o terminologías (titular de la tarjeta de pago por la del consumidor y usuario titular de la tarjeta)[605] y la inclusión del vocablo empresario, pero la redacción de ambos preceptos son idénticas.

---

buena fe que actúa conforme a las normas", en MSRBE del 2008, pp. 223 y ss*;* véanse, MARTÍNEZ NADAL, A. «El pago con tarjeta…», *op., cit*., pp. 40-48; FERNÁNDEZ-ALBOR BALTAR, Ángel. "Contratación electrónica en Internet", en GÓMEZ SEGADE, José Antonio (dir). *Comercio electrónico en Internet.* Madrid: Marcial Pons, 2001, pp. 299 y ss; vid. BUSTO LAGO, J. M (coord.). *Reclamaciones de…op., cit.,* p. 746; PLAZA PENADÉS, J.: "Cuestión de Derecho privado", en PLAZA PENADÉS, J. (coord.). *Cuestiones actuales de derecho y tecnologías de la información y la comunicación (TICS).* Monografía asociado a Revista Aranzadi de Derecho y Nuevas Tecnologías, núm. 4. Cizur Menor (Navarra): Aranzadi, S.A., 2006, p. 219; REYES LÓPEZ, Mario José. "Los métodos comerciales. La ley de ordenación del comercio minorista", en REYES LÓPEZ, M. J (coord). *Derecho de consumo*. 2. ª ed. Valencia: Tirant lo Blanch, 2002, p. 170; LÓPEZ JIMENÉZ, J. M. ª. *Uso ilícito de las tarjetas bancarias.* Barcelona: BOSCH, S.A., 2009, pp. 11 y ss; PANIZA FULLANA, A. *Contratación a…op., cit.*, pp. 315 y ss; LASARTE ÁLVAREZ, C. *Manual de protección…op., cit.,* pp. 220 y ss.

[605] SÁNCHEZ GÓMEZ, Amelia. "Comentario del art. 106 TRLGDCU, sobre pago mediante tarjeta", en BERCOVITZ RODRÍGUEZ-CANO, R (*Comentario del texto refundido de la ley*

Por lo tanto, se ha de resaltar que la reforma realizada por la LRLOCM, en el art. 46, que recoge el apartado primero del art.106 del TRLGDCU, se refiere a aquellos supuestos en los que el importe haya sido cargado mediante la utilización del número de la tarjeta de forma fraudulenta o indebida por una tercera persona ajena a su titular, es decir por un tercero distinto del titular, quien ha utilizado la tarjeta[606].

La anterior redacción del art.46 de la LOCM, modificada por el precepto 3 de la LRLOCM y el 106 del TRLGDCU, exigía como requisito necesario para la aplicación del apartado primero de este mismo art. 46 que el titular de la tarjeta con la que se ha realizado el pago no la hubiese presentado directamente o identificado electrónicamente[607]; sin embargo, en la nueva redacción dada por los respectivos preceptos de la LRLOCM y el TRLGDCU se suprimen dichos requisitos.

Algunos autores señalan que en el art. 46.1 LOCM se establece una tutela automática y una expectativa del titular de la tarjeta usada indebidamente[608], situaciones que conllevan que el comerciante "anule inmediatamente, sin poder discutir, en principio, si tal anulación es o no pertinente, si el comprador es o no titular de la tarjeta, si hubo o no

---

general para la defensa de los consumidores y usuarios y otras leyes complementarias. Cizur Menor (Navarra): Aranzadi, 2009, p. 1320.

[606] Según PANIZA FULLANA, se puede plantar algunos supuestos en el que: "el titular indica inconscientemente (o no) un número diferente al de su tarjeta o una tercera persona señala el número de otra sustraída o perdida", en PANIZA FULLANA, A. *Contratación a…op., cit.,* pp. 316-317, n 754; siguiendo la tesis sostenida por FERNÁNDEZ PÉREZ, quien sostiene que el cargo indebido, como se desprende del artículo, puede deberse a dos motivos diferenciados. De un lado, que se trata de un error del empresario, y de ahí que se hable de que el importe hubiese sido cargado «indebidamente». Y de otro, que el empresario cargara el importe a sabiendas de su error, al objeto de obtener un beneficio, esto es, que lo cargara de forma« fraudulenta», en FERNÁNDEZ PÉREZ. N.: "*El nuevo régimen*…"*op.cit*., p. 333.

[607] LASARTE ÁLVARES, C. *Manual de protección…op., cit.,* p. 220.

[608] Véanse MARTÍNEZ NADAL, A. « El pago con tarjeta…», *op., cit*., pp. 64 y ss; LASARTE ÁLVARES, C. *Manual de protección…op., cit.,* p. 220, para este autor, el art. 46. 1 LOCM, "se protege al titular de la tarjeta independientemente de que sea consumidor o no, sin tener en cuenta al adquirente a distancia, soportando únicamente el riesgo de estos medios de pago el proveedor".

utilización fraudulenta o si el fraude fue posible por razón imputable o no negligente del titular (quien, por ejemplo, acaso perdió la tarjeta y no comunicó dicha pérdida)"[609].

La Audiencia Provincial de Baleares(Sección 3ª) en su sentencia de 13 de marzo de 2007[610] señala que « (...) aunque la operación hubiera quedado perfeccionada por el concurso de la oferta y de la aceptación electrónicas, el hecho de que el supuesto pueda ser calificado como una venta fuera de establecimientos mercantiles, otorga al comprador el derecho de resolución antes reseñado, y si a ello añadimos que el pago se efectuó con la mera determinación del número de una tarjeta de crédito, el titular de la misma tiene derecho a pedir la anulación de la operación(...) pues el párrafo segundo del precepto indicado, tan sólo establece que cuando ocurra el evento indicado, se efectuarán a la mayor brevedad las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular respectivamente(...)».

De la situación descrita no cabe deducir "(...) sino el contrario, pues si la venta es susceptible de resolución (si se hace dentro de plazo) y además, si la transacción se efectuó con tarjeta, su titular tiene el derecho de anulación explicado, ello supone que el riesgo de la operación es asumido por el vendedor, conclusión que refuerza lo preceptuado en el párrafo segundo del artículo 46 de la citada Ley de Ordenación del Comercio Minorista, que reconoce al vendedor el derecho a ser indemnizado por los

[609] Así, el profesor PASQUAU LIAÑO, quien señala, que "el proveedor es quien tiene que extremar la cautela para que no produzca una utilización indebida o fraudulenta, pues, de lo contrario habrá de reabonar la cantidad percibida en la cuenta del titular de la tarjeta, sin poder discutir en un principio sobre las circunstancias que rodearon la utilización de la tarjeta. Y una vez producido el reabono cabrá la discusión, pero el titular de la tarjeta habrá obtenido una tutela rápida y segura", PASQUAU LIAÑO, Miguel. "Las ventas especiales. Ventas a distancia (*Comentario al art 46)",* en PIÑAR MAÑAS, José Luis y BELTRÁN SÁNCHEZ, Emilio (dirs.). *Comentarios a la Ley de ordenación del comercio minorista y la Ley orgánica complementaria.* Madrid: Civitas, 1997, p. 352.; LASARTE, C. *Manual sobre protección de… op., cit.,* pp. 220 y ss.

[610] EDJ 2007/119660.

daños y perjuicios causados si posteriormente se demostrara que quien realizó la compra fue el titular de la tarjeta, y que no hubo por tanto la utilización ilegítima alegada que había determinado la anulación del abono, efecto que sólo tiene sentido si se considera que el perjudicado por la anulación del abono es el vendedor".

En el mismo sentido, afirma dicho tribunal en su sentencia de 24 de mayo de 2007[611], que si «el pago se efectuó con la mera determinación del número de una tarjeta de crédito, el titular de la misma tiene derecho a pedir la anulación de la operación, sin que esté obligado, porque la Ley no lo prevé, a justificar razón alguna, pues el párrafo segundo del precepto indicado, tan sólo establece que cuando ocurra el evento indicado, se efectuarán a la mayor brevedad las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular respectivamente».

4.6.2. La exigencia de la inmediata anulación del cargo

Según se prevé en el art. 106 TRLGDCU, el consumidor y usuario titular de la tarjeta podrá exigir la inmediata anulación del cargo. Sin embargo, el precepto no aclara el sujeto a quien debe dirigirse el consumidor y usuario titular de la tarjeta para exigir la inmediata anulación del cargo[612]. Cabe señalar que para algunos autores esa facultad de anular el cargo debe ser ejercida por el titular de la tarjeta frente al proveedor de bienes o servicios[613].

[611] *AC*\2007\1908.
[612] Vid. SÁNCHEZ GÓMEZ, A. "Comentario del art. 106…", *op., cit.*, p. 1322.
[613] A favor de esta tesis véanse BERCOVITZ RODRÍGUEZ-CANO, R. "Venta a distancia…"*op., cit.,* p. 729; PASQUAU LIAÑO, M. "Las ventas especiales…"*op., cit*., p. 353; en contra de esta tesis vid. MARÍN LÓPEZ, Juan José. *La venta a distancia*, en *Nueva ordenación del comercio minorista en España*. Madrid: Cámara de Comercio e Industria de Madrid, 1996,

Sin embargo, hay quienes consideran que es a la entidad emisora a quien debe exigirse tal facultad[614].

Teniendo en cuenta los criterios sostenidos por algunos sectores de la doctrina hemos de señalar que, en realidad, es frente a la entidad emisora a quien debe dirigirse el consumidor y usuario titular de la tarjeta para exigir la inmediata anulación de cargo, no frente el proveedor de bienes o servicios.

Tanto el art. 46 de la LOCM, derogada por la LRLOCM, como el precepto 106 TRLGDCU no exigen comprobación alguna de la existencia del error para obligar al proveedor de bienes o servicios a la anulación inmediata del cargo. Lo cierto es que dicha situación puede dar lugar a un abuso, por parte del comprador a cuya tarjeta se cargó correctamente el precio, ya que éste puede exigir la inmediata anulación del cargo y conseguirlo, puesto que él no tiene que acreditar nada, ni el vendedor puede refutar nada para evitarlo[615]. Pero se podrá reclamar al titular si la anulación es fraudulenta.

[614] Siguiendo la tesis sostenida por MARTÍNEZ NADAL, tras señalar que, "la nueva redacción del art. 46 (modificado por Ley 47/ 2002 LRLOCM) no aclara este punto, por nuestra parte, como hemos puesto de manifiesto en reiteradas ocasiones, consideramos que, en realidad, es frente a la entidad emisora a quien debe (o cuanto menos puede) ejercerse tal facultad, por cuanto, en primer lugar, el art. 46 no se pronuncia expresamente sobre el sujeto, con lo que deja abiertas las puertas a otras posibilidades; en segundo lugar, porque en casos de pérdida o extravío en el comercio tradicional, es jurisprudencia consolidada que el titular de la tarjeta se relaciona directamente con la entidad emisora; además, en tercer lugar, como argumento de conveniencia u oportunidad, ello es especialmente adecuado en caso de comercio electrónico (…, por ejemplo, en el caso del titular de tarjeta español que recibe un cargo no autorizado procedente de amazon.com, ¿debe ponerse en contacto con esa empresa americana si le resulta más sencillo hacerlo con la sucursal más próxima de la entidad bancaria emisora con la que además tiene una relación contractual?)"; en cuarto y último lugar, es la entidad bancaria la única que puede proceder a ejecutar las actuaciones a que se refiere el art. 46 (las correspondiente anotaciones de adeudo y abono)", en MARTÍNEZ NADAL, A. "Atribución de responsabilidad…" *op., cit*., p. 219.

[615] BERCOVITZ RODRÍGUEZ-CANO, R. "Venta a distancia…"*op., cit.,* pp. 727-729; vid. CLEMENTE MEORO, M. "La contratación electrónica*",* en REYES LÓPEZ, María José (coord*.). Derecho de consumo.* 2ª ed. Valencia: Tiran lo Blanch, 2002, p.192*;* vid. FERNÁNDEZ-ALBOR BALTAR, Á. "Contratación electrónica…"*op., cit.,* pp. 299 y ss; PASQUAU LIAÑO, M. "Las ventas especiales…"*op., cit*., p. 352.

4.6.3. La distribución del riesgo por el uso indebido o fraudulento de la tarjeta en el comercio electrónico

Hablando del riesgo por el uso indebido o fraudulento de la tarjeta en el comercio electrónico, hemos de plantear el siguiente interrogante: ¿quién debe soportar el riesgo de aquellas operaciones llevadas a cabo en Internet, en las que se utilizaron tarjetas de crédito, cuyo número de identificación, aun siendo correcto, no ha sido facilitado por su legítimo titular sino fraudulentamente por terceros que, aparentando serlo, lo obtuvieron de manera ilícita e indebida? A nuestro juicio, el riesgo de la utilización fraudulenta o no autorizada derivado del uso de la tarjeta como medio de pago en las ventas a distancia[616], debe atribuirse al comerciante[617].

Sobre este aspecto resulta clarificatoria las sentencias mayoritarias de los tribunales españoles tras considerarse que quien debe soportar el riesgo derivado del uso indebido o fraudulento del número de la tarjeta en las ventas electrónicas es el proveedor de bienes o servicios (comerciante). Es el caso de las sentencias de la Audiencia Provincial de Barcelona (Sección 1.ª), de 22 de diciembre de 2004[618], y (Sección 19ª), de 27 de octubre de 2004[619], de, de la de Valencia (Sección. 9ª) de 17 de mayo de 2006[620], de la

[616] Según la definición dada por el apartado primero del art. 38 de la LOCM, se «considera venta a distancia las celebradas sin la presencia física simultanea del comprador y del vendedor, siempre que su oferta y aceptación se realicen de forma exclusiva a través de una técnica cualquiera de comunicación a distancia y dentro de un sistema de contratación a distancia organizado por el vendedor».

[617] PASQUAU LIAÑO, M. "Las ventas especiales…"*op., cit*., p. 353; vid. DE MIGUEL, A.: *Derecho privado…op., cit.,* p.374; vid. DOMÍGUEZ LUELMO, Andrés. "Contratación electrónica con consumidores", en MATA y MARTIN, R. M (dir.). *Los medios electrónicos de pago. Problemas jurídicos.* Granada: Comares, 2007, p. 125; PACHECO CAÑETE, M.: «La protección del consumidor una vez perfecto el contrato en las ventas de productos a distancia a través de Internet», *La Ley,* núm. 15184, 15 noviembre 2000, p. 3; SÁNCHEZ GÓMEZ, A. "Comentario art. 106 pago mediante tarjeta", en BERCOVITZ RODRÍGUEZ-CANO, R (dir.). *Comentario del texto refundido de la ley general para la defensa de los consumidores y usuarios y otras leyes complementarias*. Cizur Menor (Navarra): Aranzadi, 2009, p. 1317.

[618] *AC* 2005/90.

[619] *JUR*\2005\7712.

[620] *AC*\2006\1647.

de Jaén (Sección 1ª) de 20 de marzo de 2007[621], de la de Alicante (Sección 8ª), de 17 de julio de 2008[622], la SAP de Navarra (Sección 3ª), de 19 de junio 2008[623]; En dichas sentencias, los tribunales resuelven el fondo basándose en el contenido del contrato suscrito entre las partes, así como en lo establecido por el art.46 LOCM derogada[624].

En este sentido, la ya mencionada SAP de Barcelona (Sección 1ª) de 22 de diciembre de 2004[625], resuelve un caso relacionado con la devolución de la cantidad que había sido cargada a la cuenta de un empresario, por la retrocesión de una operación de venta efectuada a través del software de la entidad bancaria demandada. En virtud del contrato celebrado entre las partes litigantes el 24 de mayo de 2004, el proveedor de bienes o servicios se adhería al programa del comercio electrónico de la entidad bancaria.

La cuestión debatida en este procedimiento es la determinación de la persona que asume el riesgo de la operación referida en el caso de que el titular de la tarjeta rechace el adeudo, bien por robo de la misma bien por su utilización fraudulenta. Ante esta situación, la Audiencia afirma que el riesgo derivado de la utilización de las tarjetas de crédito no debe ser asumido por el titular de la misma, siempre que haya actuado con la debida diligencia, sino por el proveedor de bienes o servicios. El tribunal basa su argumento en el art. 46.1 LOCM.

Por su parte, la Audiencia Provincial de Islas Baleares (Sección 3ª), en

621 *PROV* 2007, 214499.
622 AC/2008/2380.
623 JUR\2009\43906.
624 FERNÁNDEZ PÉREZ. N.: "*El nuevo régimen…"op.cit.,* pp. 338 y ss.
625 *AC,* 2005/90; sobre estas resoluciones véanse los comentarios hechas por los siguientes autoras en sus respectivas obras: GÓMEZ MENDOZA, M.: "Comercio electrónico…"*op., cit.,* pp. 236 y ss; MARTÍNEZ NADAL, A.: "Atribución de responsabilidad…"*op., cit.,* 2007, pp. 222 y ss; RODRÍGUEZ DE LAS HERAS BALLELL, T. "El reparto de riesgo…"*op., cit.,* p. 356.

sentencia de 24 de mayo de 2007[626], resuelve una demanda presentada por

[626] Por otra parte, según establece este tribunal en su Fundamento de Derecho Segundo: «en su reciente sentencia de 13 de marzo de 2007, este mismo tribunal ha indicado, en un proceso en el que, al igual que en el presente, se invocaba la sentencia de esta misma Sala, de 4 de 28 de m ayo de 2 004 (PROV 2004, 176397), que no pr ocede aplicar la doctrina contenida en la misma y que recoge la jurisprudencia según la cual el riesgo derivado de la utilización de las tarjetas de crédito no debe ser asumido por el titular de la misma siempre haya actuado con la debida diligencia, cuando, como ocurre en el supuesto de autos, la relación jurídica objeto del proceso no es la propia de tarjeta de crédito, la cual se da entre el emisor de la tarjeta y el titular de la misma, sino la que media entre el establecimiento (...), y la entidad crediticia (...), en l a medida en que ambas partes concertaron el contrato de referencia, a través de cuya suscripción el establecimiento pretendía facilitar a sus clientes la adquisición de los servicios propios de su comercio».

Por otra parte, señala la Audiencia que, en efecto, la doctrina que desplaza los riesgos de la mala utilización de l a tarjeta a l a entidad o b anco emisor no r esulta de aplicación cuando, como ocurre en el presente caso, el objeto del proceso no son los derechos y obligaciones que deriven de las relaciones entre la entidad que emitió la tarjeta de crédito y el titular suscribiente de la misma, sino las relaciones derivadas del contrato que las partes ahora litigantes suscribieron, y que v incula al denominado "adquirente" normalmente, el banco del comerciante, y a éste, en virtud de las cuales dicho adquirente proporciona al comerciante los servicios de procesamiento que permiten el pago a través de la tarjeta, y a cambio el comerciante abona una comisión de descuento.

Para este tribunal lo esencial es determinar a q uién corresponde soportar las consecuencias de la retrocesión de los abonos efectuados en la cuenta de la parte demandada.

En este sentido, sostiene que acorde a lo establecido en las condiciones generales del contrato de af iliación al sistema Terminal de P unto de Venta (TVP) bonificado, de 27 de mayo de 2004, "en caso de incumplimiento de las obligaciones previstas en es tas condiciones el establecimiento será responsable de los quebrantos que se produzcan si el banco emisor de la tarjeta que figure utilizada no admite el cargo de la operación".

La Audiencia resaltar que quien debe asumir el riesgo en el supuesto de que la operación de pago no se haya realizado con cumplimiento de los requisitos establecidos en el contrato de afiliación al sistema TPV, es el establecimiento comercial.

Además, rechaza las alegaciones de la parte apelante, quien sostiene que la atribución del riesgo al comerciante o vendedor sea abusiva. Y a continuación, cita a esta misma Sala, en su mencionada sentencia de 13 de marzo del 2007, en la que se expresa que «el hecho de que esta asunción de responsabilidad esté inserta en un contrato típico de adhesión, que tiene la naturaleza indudable de una condición general aplicable a todas las relaciones que con idéntica causa surgen en el tráfico bancario (...) no es abusiva, antes al contrario, se ajusta a lo previsto en las leyes para tales supuestos». El tribunal entiende que, en efecto, es cierto que, como alega la parte apelante, el contrato de tarjeta de crédito no está regulado. Sin embargo, sí existen algunas disposiciones legales que arrojan luz sobre la distribución de riesgos entre los agentes intervinientes en un sistema de pago con tarjetas.

Así, como se decía en la misma sentencia de 13 de marzo de 2007 en la regulación legal de la denominada contratación a distancia en la que, precisamente con el objeto de facilitar al comprador el derecho a examinar las características del bien adquirido, se le concede el de desistir libremente de s u contratación dentro de un determinado plazo, tal y como así resulta de lo dispuesto en la LOCM(RCL 1996, 148 y 554), modificada por la Ley 47/2002, de 19 de diciembre (RCL 2002, 2980), de r eforma de la Ley 7/96, de 15 d e enero, de Ordenación del Comercio Minorista, para su adaptación al derecho comunitario, concretamente para la introducción de la Directiva 97/7 (LCEur 1997, 1493) de venta a

el Banco de Crédito Balear contra el establecimiento comercial "Viajes Amaltea, SA", en la que la entidad bancaria reclama a este último el importe correspondiente a cantidades que fueron retrocedidas, es decir, sumas que dicho banco, actuando como adquirente o banco del comerciante, no ha podido cobrar de la entidad emisora como consecuencia del uso fraudulento de una tarjeta de crédito falsificada en el establecimiento del comerciante demandado en el que no se siguió la operativa propia del sistema "TPV" establecida en virtud de contrato de 27 de junio de 2004, firmado entre las

---

distancia.

En atención a lo expuesto, y aunque la operación hubiera quedado perfeccionada por el concurso de la oferta y de la aceptación electrónicas, el hecho de que el supuesto pueda ser calificado como una venta fuera de establecimientos mercantiles, otorga al comprador el derecho de resolución antes reseñado, y si a ello añadimos que el pago se efectuó con la mera determinación del número de una tarjeta de crédito, el titular de la misma tiene derecho a pedir la anulación de la operación, sin que esté obligado, porque la Ley no lo prevé, a justificar razón alguna, pues el párrafo segundo del precepto indicado, tan sólo establece que cuando ocurra el evento indicado, se efectuarán a la mayor brevedad las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular respectivamente.

Según sostiene la Audiencia , "si la venta es susceptible de resolución (si se hace dentro de plazo) y además, si la transacción se efectuó con tarjeta, su titular tiene el derecho de anulación explicado, ello supone que el riesgo de la operación es asumido por el vendedor, conclusión que refuerza lo preceptuado en el párrafo segundo del artículo 46 de la citada Ley de Ordenación del Comercio Minorista, que reconoce al vendedor el derecho a ser indemnizado por los daños y perjuicios causados si posteriormente se demostrara que quien realizó la compra fue el titular de la tarjeta, y que no hubo por tanto la utilización ilegítima alegada que había determinado la anulación del abono, efecto que sólo tiene sentido si se considera que el perjudicado por la anulación del abono es el vendedor".

Según la tesis sostenida por la Audiencia, "está justificado si se tiene en cuenta que es el comerciante y no la entidad bancaria en que se efectúan las anotaciones contables de la operación, el único que puede tomar precauciones para evitar la utilización fraudulenta de tarjetas, entre otras, comprobar que el servicio se efectúa a quien es el verdadero titular de la tarjeta con que se hizo el pago".

Según destaca la Audiencia, que el uso de las transacciones como la que aquí se examina no sólo son beneficiosas para la entidad bancaria que cobra una comisión por cada operación realizada, sino también para los empresarios, que pueden acceder a mercados inicialmente no accesibles a través del sistema de contratación convencional; y que el comerciante es un profesional que debe saber cómo manejarse y desenvolverse en su actividad mercantil, no siendo de recibo el argumento de que ignoraba cómo funcionaba el sistema de Terminal Punto de Venta. El tribunal considera que la supresión del PIN no supone una merma de la seguridad producida sino que desde el inicio de las relaciones entre adquirente y comerciante el PIN no existía, por lo que ninguna responsabilidad especial puede recaer en el banco del comerciante ni en la entidad emisora por la supresión de dicho número de seguridad. Por lo que, se desestima el recurso de apelación interpuesto por la entidad comercial (Viajes Amaltea, SA). *(AC*\2007\1908).

partes.

Para este tribunal lo esencial es determinar a quién corresponde soportar las consecuencias de la retrocesión de los abonos efectuados en la cuenta de la parte demandada.

Según destaca la Audiencia, quien debe asumir el riesgo en el supuesto de que la operación de pago no se haya realizado con cumplimiento de los requisitos establecidos en el contrato de afiliación al sistema TPV, es el establecimiento comercial. Por tanto, le hace responsable ante el riesgo derivado de las ventas fraudulentas o indebidas.

En parecidos términos, la SAP de A Coruña (sección 5ª), de 25 abril de 2006[627] resuelve un conflicto que tiene su origen en un litigio mantenido

[627] Al respecto, el tribunal señala que se hace expresamente responsable al "establecimiento" «en el caso de recibir el banco la comunicación de un cliente solicitando la anulación del cargo, o de haber devuelto la mercancía, no haberla recibido o haber causado baja, el banco queda facultado para considerar anulada la factura original y cumplimentar la correspondiente nota de abono, con cargo a la cuenta que mantenga el establecimiento con el banco».

Según la Audiencia, «la referida asunción del riesgo de las operaciones de venta realizadas a través del sistema de pago que para el comercio electrónico le facilita al comerciante la entidad bancaria, por aquél resulta también de lo que, en forma clara y concluyente, sin duda alguna susceptible de interpretación, dispone la condición general 8ª del referido contrato de comercio electrónico, a tenor de la cual si el cliente afirma no haber recibido la mercancía/servicio o, por cualquier razón, devuelve uno o varios de los productos solicitados con el fin de cancelar total o parcialmente su pedido, el Establecimiento queda obligado a realizar la operación correspondiente a través del sistema informático, no pudiendo, por tanto, efectuar reembolsos de dinero en efectivo por devoluciones de mercancías abonadas con tarjeta».

Al tiempo que, en virtud de la condición general 9ª, se faculta al Banco, «en caso de recibir (...) comunicación de un cliente solicitando la anulación del cargo, o de haber devuelto la mercancía, no haber la recibido o haber causado baja», para considerar «anulada la factura original y cumplimentar la correspondiente Nota de Abono, con cargo a la cuenta que mantenga el establecimiento con el banco»; a la vez que la ya referida estipulación 4ª del "Anexo de venta por correo (...)" contempla la obligación del establecimiento, para el caso de que la Entidad emisora de la Tarjeta utilizada como medio de pago devolviera la transacción por cualquier causa a «reponer su importe a le entidad financiera con la que inicialmente liquidara la factura de venta original», siendo en este caso de aplicación la estipulación 3ª del Anexo, similar a la transcrita condición general 9ª del contrato de comercio electrónico.

Por su parte, este tribunal señala que «estamos en presencia de pactos de imputación de responsabilidad civil al comerciante--el denominado "Establecimiento"- que utiliza este

entre la entidad comercial, ahora recurrente, afiliada al sistema de pago con tarjeta de crédito, cuya actividad consistía en vender productos a través del comercio electrónico, y una entidad bancaria (Banco Español de Crédito, S.A) que es proveedor del mecanismo de pago (TPV Virtual).

La cuestión que se plantea a la decisión de la sala no es otra que la de determinar quién debe asumir los riesgos derivados de l a utilización fraudulenta de tarjetas de crédito para realizar el pago de los productos vendidos a través del comercio electrónico por la entidad adherida o afiliada a dicho sistema.

Para el tribunal, el riesgo económico derivado de las tres operaciones de venta fallidas -en una de la cuales, la de mayor valor económico, no resulta siquiera acreditado que se haya entregado la cosa objeto de l a misma al pretendido adquirente o comprador- debidas a un uso fraudulento de tarjetas de crédito utilizadas como medio de pago y que constituyen el fundamento de la acción de reclamación de cantidad ejercitada por la entidad recurrente, sería a c argo del establecimiento, sin poder trasladarlo a la entidad financiera demandada. O sea, el tribunal señala que dicho riesgo es imputable al proveedor de bienes o servicios a través del comercio electrónico.

Así lo ha expresado la Audiencia Provincial de Asturias (Sección 6ª) en

---

sistema de cobro y que vienen justificados por la propia mecánica de este tipo de operaciones caracterizada porque el abono en cuenta del importe inicial de la factura se hace de manera automática a partir de los datos de la tarjeta de crédito facilitados por el comprador. Pactos de asunción previa de responsabilidad del buen fin de la operación por el comerciante o proveedor que son conformes con la regulación legal de la contratación a distancia en la que, precisamente con el objeto de facilitar al comprador el derecho a examinar las características del bien adquirido, se le concede el de desistir libremente de su contratación dentro de un determinado plazo, tal y como así resulta de lo dispuesto, entre otros, en el art. 44 de la Ley de Ordenación del Comercio Minorista (Ley 7/1996, de 15 de enero), modificada por la Ley 47/2002, de 19 de diciembre, para su adaptación al derecho comunitario, en particular para integrar las exigencias de la Directiva 97/7, de venta a distancia».
JUR \2007\135035.

la sentencia de 14 de marzo de 2005[628] tras sostener que el proveedor de bienes o servicios es quien debe asumir la responsabilidad del buen fin de la operación.

En este sentido, el órgano judicial expresa que, el único que puede tomar precauciones para evitar la utilización fraudulenta de tarjetas y de comprobar que la entrega de la mercancía se efectúa a quien es el verdadero titular de la tarjeta con que se hizo el pago, es el proveedor de bienes o servicios.

Del mismo parecer, la SAP de Madrid (Sección 12ª) de 4 marzo de 2008[629], que resuelve un caso basado en la acción de reclamación de cantidad de 73.592,71.-€ deducida por el BBVA, contra la parte apelante. Según señala el tribunal, el objeto de la reclamación son los abonos previos de ventas llevadas a cabo por el establecimiento demandado a través de Internet, cuyos pagos se efectuaban por tarjetas de crédito VISA y MASTER. Resulta que el 12 de febrero de 2002 la empresa "FUTBOL DETUP, S.L.", firmó un contrato de afiliación a los sistemas de tarjetas relativo a las ventas presenciales o por Internet de sus productos[630].

---

628 (*JUR*\2005\89982).

629 (*JUR*\2008\191298).

630 Expresa la sentencia de referencia que en "dicho contrato la sociedad demandada se comprometió a satisfacer al banco las devoluciones de remesas que, como consecuencia de sus operaciones de venta de mercancías, pudieran producirse. Que este contrato es el que regía las relaciones entre las partes se ve confirmado por el hecho de que el 14 de octubre de 2003 el Administrador de la empresa envía al Banco un documento requiriendo el cambio de pago de tarjeta "3 D SECURE" al de tarjeta tradicional que evidentemente ofrece menos seguridad en las transacciones. A raíz de ello se produce un incremento extraordinario de las ventas, y el 11 de febrero de 2004 el Administrador reclama la activación del protocolo de seguridad "3D SECURE" el mismo que cuatro meses antes había exigido que se le retirara. Como consecuencia de las ventas realizadas en Internet entre el 26 de diciembre de 2003 y 11 de febrero de 2004, el Banco abonó en la cuenta de la demandada la cantidad de 73.592,71€, importe del que la empresa dispuso efectivamente".

Añade la Audiencia, que «todas y cada una de las transacciones cuyo importe asciende a la cantidad expresada, fueron posteriormente anuladas y dejadas sin efecto por los supuestos compradores de la hoy apelante y titulares de las tarjetas de crédito, alegando uso fraudulento de las mismas, por lo que el Banco tuvo que reintegrar las cantidades cargadas en las tarjetas a las entidades emisoras y por consiguiente a dichos titulares,

En relación al orden de la imputación de responsabilidad en las operaciones fallidas debidas a un uso fraudulento de tarjetas de crédito utilizadas como medio de pago, sería el comerciante quien debe asumir dicha responsabilidad, sin poder trasladarla a la entidad financiera demandada.

Por último, la Audiencia sostiene que "el hecho de que las entidades financieras cobren una comisión por cada operación realizada con tarjeta de crédito, en nada modifica la responsabilidad del comerciante ya que ello es una contraprestación por tal servicio pero por sí solo no justifica el hacerles cargar con las consecuencias de un uso fraudulento, cuando como aquí acontece se asume en el contrato por los comerciantes o empresarios, que también se benefician de este sistema de ventas, la responsabilidad del buen fin de la operación"[631]. Por esta razón, el tribunal desestima el recurso

---

como se acredita en los expedientes que se adjuntan con la demanda, en cada uno de los cuales figuran todos estos datos. De acuerdo con lo establecido en el contrato, la Empresa tiene la obligación de devolver a la actora las cantidades reintegradas por ésta a los auténticos titulares de las tarjetas de crédito utilizadas para realizar las compras».

[631] Afirma el órgano judicial que esos pactos de imputación de responsabilidad al comerciante que utiliza este sistema de cobro vienen justificados por la propia mecánica de este tipo de operaciones, caracterizada porque el abono en cuenta del importe inicial de la factura se hace de manera automática a partir de los datos introducidos, esto es sin otra comprobación que el límite de crédito de la tarjeta y su fecha de caducidad.

Al mismo tiempo, añade que "los pactos de asunción previa de responsabilidad del buen fin de la operación por el comerciante o proveedor son conformes con la regulación legal de la denominada contratación a distancia en la que, precisamente con el objeto de facilitar al comprador el derecho a examinar las características del bien adquirido, se le concede el de desistir libremente de su contratación dentro de un determinado plazo, tal y como así resulta de lo dispuesto, entre otros, en el art. 44 de la Ley de Ordenación del Comercio Minorista , modificada por la Ley 47/2002, de 19 de diciembre, de reforma de la LOCM 7/96, de 15 de enero, para su adaptación al derecho comunitario, concretamente para la introducción de la Directiva 97/7 de venta a distancia, estableciendo la misma LOCM, en su art. 46.

Al respecto, dicha normativa establece que cuando se trata de la venta a distancia con pago por medio de la tarjeta «la responsabilidad del buen fin de la operación es del proveedor, de ahí la adaptación a la misma de las condiciones recogidas en el contrato de tarjeta de crédito litigioso, estando la misma justificada si se tiene en cuenta que es el citado y no la entidad bancaria en que se efectúan las anotaciones contables de la operación, el único que puede tomar precauciones para evitar la utilización fraudulenta de tarjetas, de comprobar que la entrega de la mercancía se efectúa a quien es el verdadero titular de la

de apelación interpuesto por el establecimiento comercial, y se le atribuye la responsabilidad derivada del uso indebido o fraudulento.

En sentido contrario, en una línea jurisprudencial que consideramos minoritaria, cabe citar la Sentencia de la Audiencia Provincial de Madrid (Sección 11ª) de 23 de abril de 2004[632], tras resolver un caso basado en un contrato de afiliación a los sistemas de tarjetas de crédito para las operaciones de venta no presencial, suscrito entre Bankia y el Comercio, que no comparte las tesis sostenidas por las sentencias que hemos comentado a lo largo de este epígrafe.

Así pues, el origen de esta demanda versa sobre el presunto error de hecho en la interpretación de la prueba, porque según sostiene la parte apelante en la sentencia, no se realiza un enfoque «sociológico», ni «analógico» según lo establecido en los arts. 3.1 y 4 del C.C., porque entiende que el contrato de 5 de diciembre de 1997 aplicó el clausulado de las ventas no presenciales efectuadas por correo, que era el único previsto hasta entonces, a las realizadas por teléfono, modalidad no regulada contractualmente por la entonces apelante [633].

Según pone de manifiesto el tribunal, otra de las circunstancias a tener en cuenta en este caso, es la retrocesión, que conforme al art. 46.1º de la LOCM (RCL 1996, 148, 554), se define como el derecho del titular de la

tarjeta con que se hizo el pago».

[632] (JUR 2004\228548).

[633] Según la tesis sostenida por la Audiencia en el Fundamento de Derecho Segundo, se «distingue perfectamente entre el contrato citado de 5 de diciembre de 1997, que es el determinante de la reclamación de cantidad, y el de 1 de marzo de 2002, en que se modernizó el sistema de comisión, reduciéndose la anterior «de lujo», según la descripción de la empleada de la recurrente, que intervino en la contratación, pues ascendía al 5,5%, pasando a ser en el nuevo contrato del 2,75%, con la exención de responsabilidad de la entidad crediticia por el buen fin de la operación, no especificada dicha cláusula, en el contrato anterior, que sólo preveía la expresión «salvo buen fin» para el supuesto de venta por correo. Siendo aquella comisión incluso mayor que la aplicada en las operaciones de venta presencial».

tarjeta a anular el cargo realizado por otra persona sin su consentimiento al operador crediticio. El riesgo de esta operación debe imputarse según las cláusulas del contrato de afiliación de tarjetas al operador bancario o al cliente. De este modo, el tribunal señala que el primer contrato de 5 de diciembre de 1997 no precisaba exoneración de responsabilidad de la demandada para la retrocesión, de ahí la elevada comisión cobrada, pues se perfilaba a cargo de la misma. Sin embargo, en el segundo contrato, como indica esta Audiencia, sí se establece expresamente la exoneración para el operador financiero, con rebaja de la comisión a la mitad.

Al respecto, se establece en el Fundamento de Derecho Tercero, que «en el contrato suscrito entre las partes, no se preveía estipulación alguna, para el supuesto de la exención de responsabilidad de la parte demandada (Caja Madrid), respecto de las ventas por teléfono, porque la cláusula de estilo «salvo buen fin» sólo se aplicaba a las ventas por correo. A cambio la comisión cobrada por «Caja Madrid», era del 5,5%, en general, para todas las operaciones de venta no presencial, el doble que la del 2,5%, percibida por las de venta presencial».

Al mismo tiempo, resalta que "no se puede exigir al establecimiento comercial la mayor diligencia en su gestión, teniendo en cuenta las circunstancias de sus operaciones, las cuales quedan conectadas con la entidad emisora de la tarjeta, a fin de obtener la previa conformidad de la operación de venta por teléfono, de un surtido de productos ofrecidos mediante catálogo tangible, o por Internet, y abonar la correspondiente comisión, además del ya citado pago en cuenta, que comporta el beneficio para la Caja, todo ello dentro de lo que se denomina contrato de afiliación de la tarjeta".

En este sentido, el tribunal rechaza la exoneración implícita que pretende la parte demandada, por la vía de la interpretación «sociológica» y

«analógica», tras poner de manifiesto que no es admitida en este caso porque es preciso que se hubiera expresamente pactado, apoyándose, en este caso, en la, en la STS de 8 de marzo de 1990 (RJ 1990, 1679), y en la regulación del art. 5.1º, párrafo 2º de la LCG.

Por esta razón, la Audiencia desestima el recurso de apelación interpuesto por la entidad bancaria, argumentando que ésta debe soportar el riesgo inherente a los referidos pagos.

En posición similar parecen pronunciarse la Audiencia provincial de Cáceres (Sección 1ª) en su sentencia de 28 de enero de 2004[634]; y el Juzgado de Primera Instancia núm. 7 de Guipúzcoa, Donostia-San Sebastián, de 13 de octubre de 2004[635]. Este último analiza un contrato de cuenta corriente suscrito entre las partes para operar utilizando un sistema de tele pago comercializado por la propia entidad bancaria y denominado TPV, por cuya utilización la enditad bancaria cobraba una comisión.

Al respecto, señala el Juzgado que «el fondo de la controversia gira en torno a la seguridad de los pagos». Según sostiene el Juzgado, "el demandado había alcanzado una convicción de que los pagos realizados y anotados en cuenta por el Banco ya tenían una comprobación inicial de que eran válidos porque se abonaban por tarjeta, de tal forma que al abonar las cantidades en la cuenta del demandado, éste estaba en la creencia de que dicho pago era cierto y definitivo y, por ello, una vez recibido el dinero, enviaba mediante mensajero el producto encargado al destinatario".

Por su parte, la entidad bancaria alega que no asume ningún riesgo en la gestión del cobro, sino que se limita a poner un sistema en funcionamiento

[634] Esta sentencia fue analizada por GÓMEZ MENDONZA, M. "Comercio electrónico…"*op., cit.,* pp. 240 y ss; y MARTÍNEZ NADAL. A.: "Atribución de responsabilidad…"*op., cit*., p. 221.

[635] Sentencia núm. 195/2004, de 13 de octubre de 2004, Procedimiento núm.

de tal forma que adelanta el pago para que su cliente disponga antes del dinero y espera a ver si se cobra, de tal forma que, si el banco no recibe el dinero, traslada la obligación de pago a su propio cliente.

Sin embargo, el Juzgado sostiene que en el contrato se recoge que el Banco, excepcionalmente, puede realizar operaciones que se califican como «a buen fin», es decir, operaciones que son de especial riesgo, y en las que su propio cliente asume el riesgo. A pesar de no haberse cumplido todos y cada uno de los requisitos el establecimiento decide efectuarlas bajo su propio riesgo y en el bien entendido de que deberá soportar el adeudo de su importe si el emisor de la tarjeta no admite el cargo de la operación.

Añade la Instancia que cuando se trata de una operación de las que se califican como «a buen fin» el cliente debe conocer esta situación antes de realizar la operación de venta para salvaguardar sus intereses.

En este sentido, señala el Juzgado que en estos casos y excepcionalmente, es el cliente el que asume el riesgo de impago, mientras que en el resto de casos es el Banco el que lo asume. Ciertamente, el Banco tiene acceso a información de otros bancos, celebra acuerdos con ellos, puede comprobar el saldo o la realidad de una tarjeta que se utiliza para el pago, etc., es decir, tiene medios para verificar el riesgo de la operación y para advertir al cliente de que esa operación no es viable, debiendo ser dicha reacción automática.

De acuerdo con los argumentos sostenidos por el Juzgado, éste desestima la demanda presentada por el banco, alegando lo siguiente:

> «La reclamación que realiza el banco en este procedimiento se centra básicamente en el contrato que realizaron banco y cliente. Sin embargo,

> nada hace pensar que dicho contrato ampare una reclamación como la que se realiza a través del presente procedimiento, dado que el cliente actuó en su legítima creencia, amparada por el comportamiento del banco en todo momento, de que el medio de pago era seguro en el sentido de que una operación que el banco procedía a anotar en cuenta suponía que el Banco emisor de la tarjeta había emitido una confirmación sobre el saldo existente en la misma, y de ninguna manera iba a repercutir en el propio cliente del banco el pago de la cantidad reclamada».

Por su parte, la Audiencia Provincial de Barcelona (Sección 1ª) en su sentencia de 4 de mayo de 2010 [636] resuelve un caso relacionado con la suscripción de un contrato de "Afiliación Comercio al sistema de Tarjetas Genérica Visa", a través del cual la entidad bancaria ofrecía un servicio de gestión de cobros y pagos realizados a través de tarjetas, mediante la adhesión del establecimiento al servicio Tele pago 4B (TPV), pero que se habían producido una serie de devoluciones porque el banco emisor de las tarjetas rechazaba el efectivo abono, alegando que la operación no fue realizada ni autorizada por el titular, generándose de este modo a favor de la demandante un saldo de 17.864,21 euros cuya reclamación constituye el objeto del presente litigio.

---

[636]. También sostiene que la parte demandada disponía de una opción denominada "Consulta de operaciones", que le permitía controlar sus ventas y a través de la que podía conocer los datos que se recogen en el documento 11 de la demanda, esto es, la referencia de la venta, la fecha, hora y número de autorización, y lo que es más importante, si la operación había sido realizada de forma segura (CES) o de forma no segura (SSL).

Según expresa el tribunal que "está admitido que se efectuaron compras electrónicas con la utilización de tarjetas que no fueron admitidas por sus titulares, de manera que fueron los propios titulares quienes exigieron la anulación del cargo, lo que fue aceptado por las entidades bancarias, de conformidad con lo preceptuado en el artículo 46 de la Ley 7/1996, de 15 de enero (RCL 1996, 148, 554) de Ordenación del Comercio Minorista, según la redacción que le dio la Ley 47/2002, de 19 de diciembre (RCL 2002, 2980) que traspuso la Directiva 97/7 /CE (LCEur 1997, 1493)".

Al mismo tiempo, sostiene que, es fundamental estudiar los términos del contrato, en la medida en que no se discute la procedencia de la retrocesión de la operación y el debate queda reducido a la relación contractual concertada entre las partes ahora litigantes, quedando fuera de nuestro estudio tanto la relación entre el emisor de la tarjeta y el titular de la misma como los contratos electrónicos celebrados por la demandada cuyo carácter de fraudulento no se discute. (*JUR*\2010\277548).

La Audiencia considera que lo más importante es determinar quién debe asumir el riesgo de la operación en el caso de que el titular de la tarjeta rechace el adeudo por haber sido utilizada de manera fraudulenta.

Según consta en el contrato suscrito entre las partes, en su cláusula 12 existen dos sistemas diferentes de realizar las operaciones de venta:

"1) El sistema SSL, a través del cual si el banco emisor de la tarjeta utilizada como medio de pago devolviera la transacción por cualquier causa, el establecimiento se obligaba a reponer su importe al banco con el que liquidara la factura de venta original, (en el caso de autos el Banco demandante).

2) El sistema 3D Secure/UCAF que reviste el carácter de venta con identificación del comprador titular de la tarjeta, en cuyo caso si el banco emisor de la tarjeta utilizada como medio de pago devolviera la transacción por negar el titular de la tarjeta su participación en la transacción, el establecimiento no se obliga a reponer su importe al banco con el que inicialmente liquidara la factura original".

En este sentido, el tribunal considera que era por tanto, esencial la determinación del sistema que se iba a aplicar porque de ello derivaban responsabilidades bien distintas, y porque la actuación del establecimiento era también diferente, pues en el sistema SSL era suficiente con la determinación del nombre, número de tarjeta, fecha de caducidad y cantidad, mientras que en el sistema seguro, se exige además que el establecimiento compruebe la identidad del titular que efectúa la transacción, normalmente a través de una clave o PIN o por cualquier otro modo, entre el que puede encontrarse incluso la autorización por el banco emisor de la tarjeta.

Añade la Audiencia, que no resulta por ello admisible, que la parte ahora apelante pretenda desplazar sobre el establecimiento demandado la responsabilidad por lo acontecido, pues además de que es de su cargo la inconcreción del contrato en la elección del sistema, no consta que el demandado hubiera incumplido los parámetros de seguridad a que se comprometió, ni es razonable exigirle que presumiera que el repunte de ventas experimentado fuera atribuible a actuaciones fraudulentas y no al efecto de la divulgación efectuada a través de congresos, como así refiere la legal representante de la parte demandada. Por ello considera que la entidad bancaria es quien debe responder por el uso indebido o fraudulento.

Como se ha podido comprobar a lo largo de este epígrafe existen dos vertientes en la jurisprudencia española contrapuestas, a la hora de determinar quien debe asumir el riesgo por el uso fraudulento de la tarjeta de crédito en internet.

En este sentido, de acuerdo con la jurisprudencia mayoritaria antes revisada, quien debe soportar el riesgo por el uso fraudulento de la tarjeta de crédito en internet es el proveedor de bienes o servicios (empresario); o sea, quien debe asumir la responsabilidad de las operaciones fallidas debidas a un uso fraudulento de tarjetas de crédito utilizadas como medio de pago sería el proveedor de bienes o servicios, sin poder trasladarla a la entidad financiera.

En sentido contrario, la jurisprudencia que consideramos minoritaria, hace recaer la responsabilidad de las operaciones fallidas debidas a un uso fraudulento de tarjetas de crédito utilizadas como medio de pago, en la entidad bancaria.

4.6.4. Análisis del apartado segundo del art. 106 TRLGDCU: el derecho de ejercer la acción correspondiente en reclamación de una indemnización de daños y perjuicios frente al titular

Según señala la doctrina, a pesar de lo establecido en el apartado primero del art. 106 TRLGDCU, no se quiere decir que posteriormente el proveedor de bienes o servicios no pueda ejercer la acción correspondiente en reclamación de una indemnización de daños y perjuicios frente al titular que solicitó la anulación del cargo. A estos efectos, el legislador español con tal de evitar un futuro abuso del usuario y consumidor, establece en el apartado segundo de este mismo precepto 106 del TRLGDCU que «sin embargo, si la compra hubiese sido efectivamente realizada por el consumidor y usuario titular de la tarjeta y la exigencia de devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento o de resolución, aquél quedará obligado frente al empresario al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación».

En este caso, interpretando lo establecido por el precepto, diríamos que la carga de la prueba recae sobre el proveedor de bienes o servicios, quien a la vez tiene que probar que el número de la tarjeta utilizada para pagar las compras en el comercio electrónico, o mejor dicho en Internet, ha sido introducido por el propio titular legítimo de la tarjeta, pudiendo en este caso exigir el resarcimiento del daño y perjuicio que hubiera podido ocasionarle a consecuencia de dicha anulación del cargo; es decir, en este caso, el titular no sólo se verá obligado a responder del incumplimiento de la obligación contraída, sino que estará sujeto a indemnizar al proveedor de los bienes o servicios contratados, así como por los daños y perjuicios que hubiera podido ocasionarle a consecuencia de dicha anulación[637].

[637] En la doctrina FERNÁNDEZ-ALBOR BALTAR, señala que "no sólo será exigible al titular la responsabilidad, en el caso que él personalmente hubiera realizado la transacción,

Finalmente, cabe señalar que, a la vista de todo lo expuesto en estos epígrafes, podemos concluir que lo que se anula como consecuencia de la utilización del número fraudulento o indebido de la tarjeta, no es el contrato en sí, sino el cargo que se efectúa[638].

Por otro lado, se ha de resaltar una de las novedades introducidas por el legislador español con la reforma del art. 46.1LOCM: para que el titular de la tarjeta pueda anular la operación, se exige que el uso del número de la tarjeta haya sido utilizado indebidamente o de modo fraudulento por un tercero y no por él[639]; o sea, corresponde al titular de la tarjeta probar o demostrar la existencia de una situación de fraude o de uso indebido del número de la tarjeta para así poder anular el cargo fraudulento.

También el titular de la tarjeta cuyo número ha sido utilizado fraudulenta o indebidamente por un tercero tiene derecho a exigir la anulación del cargo y la restitución de la cantidad cargada en su cuenta inmediatamente. Por lo tanto, ante la anulación de los cargos por parte del titular de la tarjeta, en

---

sino también en el caso en que hubiera realizado un tercero con su consentimiento," FERNÁNDEZ-ALBOR BALTAR, Á. "Contratación…"*op., cit*., p. 300; Según señala BERCOVITZ RODRÍGUEZ-CANO, estamos ante "un supuesto de incumplimiento contractual doloso, con las consecuencia de los preceptos 1101, 1106, 1107, párrafo 2.º, y 1124 CC., y que igualmente comprenden en todo caso la indemnización de daños y perjuicios, en lo que habrá que añadir el precio de la venta todavía impagada si el vendedor opta por el cumplimiento de la misma (art. 1124 CC.)," BERCOVITZ RODRÍGUEZ-CANO, R.: "Venta a distancia…"*op., cit.,* p. 730; CLEMIENTE MEORO, Mario. «La contratación electrónica», en *Las incorporaciones de las nuevas tecnologías en el comercio: aspectos legales. Estudios de Derecho Judicial*, núm. 71, 2006. Madrid: Consejo General del Poder Judicial pp. 131-191, en p.157; vid. MARÍN LÓPEZ, Juan José. *La venta a distancia*, en *Nueva ordenación del comercio minorista en España*. Madrid: Cámara de Comercio e Industria de Madrid, 1996, pp.167 y ss; vid. SÁNCHEZ–CALERIO G. J. «Tarjeta de crédito y tutela del consumidor», en *RDBB*, núm. 98, abril-junio, 2005, p. 114; DOMÍGUEZ LUELMO, A. "Contratación…"*op., cit*., p.126; siguiendo el criterio sostenido por LASARTE ÁLVARES, quien señala que para "la aplicación del apartado segundo del art. 46 de la LOCM, se requiere el carácter indebido de la anulación del cargo solicitada por el titular de la tarjeta así como la prueba de los daños y perjuicios causados al proveedor con dicha anulación", en LASARTE ÁLVAREZ, C. *Manual de protección…op., cit.,* p. 221; vid. CASELLAS, D. "obligaciones y responsabilidad…"*op., cit.,* p. 46.

[638] Vid. BOTANA GARCÍA, G. «Los contratos a distancia y la protección de los consumidores», en ILLESCAS ORTIZ, R (dir.). *Derecho del comercio electrónico*. Madrid: Editorial la Ley, 2001, p. 348.

[639] Vid. GÓMEZ MENDOZA, M.: "Comercio electrónico…"*op., cit.,* p. 236.

relación al uso indebido o fraudulento del número de la tarjeta en las operaciones llevadas a cabo en el comercio electrónico (Internet), quien debe soportar el riesgo de la operación comercial es el proveedor de bienes o servicios, sin que pueda entrar a valorar si efectivamente el número de la tarjeta se ha utilizado correctamente por su titular o indebidamente o fraudulentamente por un tercero.

A nuestro juicio, las dos normativas analizadas se quedaron cortas, en el sentido de que no se establece un plazo concreto para la devolución, por lo que habría que recurrir, por analogía, al precepto 104 del TRLGDCU en el que se establece un plazo que no deberá superar los 30 días desde la comunicación de la solicitud de la anulación del cargo[640]. Sobre este mismo aspecto creemos que el legislador tenía que haber establecido un plazo de forma explícita sin tener que estar usando por analogía otros preceptos.

4.7. Consideraciones finales

Como hemos podido ver a lo largo de esta investigación, uno de los mayores problemas que viene presentando el uso de tarjetas de crédito o débito en el comercio electrónico se da en el ámbito de la responsabilidad por el uso fraudulento de la misma ya que no existían regulaciones o disposiciones específicas que recogiesen de forma vinculante preceptos con el objetivo de proteger a los consumidores y usuarios de las tarjetas de crédito. Sin embargo, con la aprobación de la Ley 16/2009, de servicios de pago, el legislador español siguiendo lo establecido por el legislador comunitario en la Directiva 2007/64, sobre sistemas de pago en el mercado interior, prevé la garantía de protección al consumidor en el uso indebido o fraudulento de la tarjeta y que el límite de responsabilidad sea de obligatorio cumplimiento.

[640] Véase BERCOVITZ RODRÍGO-CANO, R.: "Ventas a…"*op., cit.*, p. 729; FERNÁNDEZ PÉREZ, N.: "*El nuevo régimen…"op., cit.,* p. 344.

Teniendo en cuenta las tesis sustentadas por las diversas sentencias de los tribunales españoles que hemos comentado en uno de los epígrafes de esta investigación, en relación con la validez de las cláusulas de exención de responsabilidad de la entidad emisora, por extravío o sustracción de la tarjeta, antes de que su titular notifique su pérdida, han de considerarse válidas dichas cláusulas, ya que se trata de cláusulas que exclusivamente exigen al titular de la tarjeta la obligación de notificar o comunicar con rapidez la sustracción, el extravío o pérdida de la tarjeta y su responsabilidad con anterioridad a la notificación .

En cambio, la Sala 1 ª de lo Civil del Tribunal Supremo, en sentencia de 16 de diciembre de 2009, califica de "abusivas, imprecisas e inciertas", todas aquellas cláusulas en las que se exige al titular notificar la pérdida, sustracción o extravío urgentemente, a la mayor brevedad, de forma inmediata, de inmediato e incluso aquella que exige que dicha comunicación o notificación se produzca antes de transcurrir 24 horas desde su acaecimiento.

Se ha de tener en cuenta que cualquier cargo que se hiciese en la cuenta del cliente tras la sustracción o extravío de la tarjeta es ajeno a la responsabilidad de la entidad emisora de la misma en tanto en cuanto no se le haya comunicado por el interesado o haya podido conocer por otro medio el hecho de su ilícita utilización.

Como se ha puesto de manifiesto en uno de los epígrafes de este capítulo existen diferentes cláusulas abusivas tales como:

- Las cláusulas de exoneración o limitación de responsabilidad de forma absoluta a la entidad emisora por fallos propios de su sistema informático o por la intromisión de terceros fuera del control del banco

- Las que eximen de total responsabilidad a la entidad emisora de manera indiscriminada y sin matización o modulación alguna.

- Aquellas que exoneran de responsabilidad en todo caso (es decir, sin tener en cuenta las circunstancias del caso concreto) a la entidad bancaria por los cargos realizados con tarjetas sustraídas antes de tener el emisor conocimiento de dicha circunstancia.

- Las que excluyen totalmente de responsabilidad para el supuesto de utilización de la tarjeta por quien no es su titular durante el tiempo que medie hasta su notificación.

- Aquellas que pretenden extender la responsabilidad del titular de la tarjeta de crédito por el uso fraudulento de la misma después de la notificación de la situación de riesgo. Consideramos que estos tipos de cláusulas son abusivas, dado que son cláusulas predispuestas y redactadas unilateralmente por la entidad emisora de la tarjeta que producen un desequilibrio de prestaciones.

Por lo tanto, cabe matizar que dichas cláusulas representan el traslado al titular de todo riesgo por el uso fraudulento de las tarjetas en el comercio electrónico, y, en efecto, deben ser consideradas nulas ya que traen consigo un desequilibrio importante de derechos y obligaciones de ambas partes en perjuicio del consumidor o usuario, al imponerse, en la práctica, una absoluta asunción de responsabilidad a cargo del titular de la tarjeta de pago en los casos de utilización de la misma y de su número secreto, y correlativamente, supone una total exclusión de responsabilidad por parte de la entidad

emisora revistiendo por ello el carácter de abusivas conforme a lo previsto por el art. 82.1, 86. 2 y 89.1 del TRLGDCU.

Coincidiendo con lo que viene sosteniendo la doctrina, cabe señalar que la declaración de una cláusula como abusiva debe instarse judicialmente, por lo que será necesario acudir a la vía jurisdiccional. Es decir, sólo un juez puede dictaminar que en un contrato determinado, una cláusula es abusiva y por tanto nula.

Asimismo, hemos de señalar que la nulidad de alguna cláusula por su carácter abusivo no determina la ilegalidad del resto del contrato por lo que en el mismo pronunciamiento judicial se deberá determinar la eficacia de las estipulaciones no afectadas.

En relación con la responsabilidad del titular, se ha de concluir que este soportará las pérdidas, extravío o robo de la tarjeta, hasta un límite máximo 150 euros, siempre y cuando aquel actúe de forma diligente es decir, sin actuar de manera fraudulenta o con negligencia grave o sin cumplir con lo establecido en la mencionada normativa.

Se ha de reseñar que la actuación negligente del titular de la tarjeta de crédito le hace responsable frente al proveedor de bienes o servicios y frente a la entidad emisora de la tarjeta, de los daños y perjuicios ocasionados; por ejemplo, por haber facilitado a un tercero los datos bancarios (número de la tarjeta, fecha de caducidad y código de seguridad), o por no haber comunicado a la entidad emisora la pérdida o extravío de la misma.

Por último, en relación con el cargo fraudulento o indebido, el párrafo primero del art. 106 del TRLGDCU, establece para los “pagos mediante tarjeta”, que “cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente, utilizando el número de una tarjeta de pago, el consumidor o usuario titular de ella podrá exigir la inmediata anulación del

cargo; En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del empresario y del consumidor y usuario titular de la tarjeta se efectuarán a la mayor brevedad".

Teniendo en cuenta lo planteado por el legislador español en el precepto que se comentó en el párrafo anterior, a nuestro juicio, éste se quedó corto en su previsión dado que no llega a establecer de forma explícita el plazo concreto para la devolución del importe cargado fraudulenta o indebidamente. Se limita a indicar que el consumidor o usuario titular de la tarjeta podrá exigir la inmediata anulación del cargo y que las correspondientes anotaciones de adeudo y reabono (…) se efectúan a la mayor brevedad posible.

En este sentido, se ha de sostener que no existe ningún precepto, tanto en la LRLOCM, así como en el TRLGDCU, que regule el plazo para que el consumidor o usuario titular de la tarjeta ejerza el derecho a reclamar la anulación del importe cargado de modo fraudulento o indebido. Ante este vacío habrá que recurrir, por analogía, al precepto 104 del TRLGDCU en el que se establece un plazo que no deberá superar los 30 días para la devolución al consumidor y usuario de las cantidades abonadas.

Por último, creemos conveniente proponer la modificación del apartado primero de este mismo art. 106 del TRLGDCU o que se añada un segundo párrafo, en el cual se establezca un plazo de 15 a 30 días para la devolución del importe cargado de modo fraudulento o indebido, evitando así la utilización de criterios por analogía, que ni siquiera abordan cuestiones relacionadas con lo señalado en el párrafo primero de este mismo art.106 del TRLGDCU.

Además, es necesario añadir un párrafo en la que se exija la diligencia del consumidor o usuario titular de la tarjeta de un uso correcto de la misma;

por ejemplo, que teniendo conocimiento de la existencia de un extravío o sustracción deba proceder diligentemente a c omunicarlo sin demora indebida, por lo que se tendrá en cuenta dicha notificación para la anulación del cargo fraudulento o indebido.

Por último, desde nuestro punto de vista, el estudio de la normativa (Europea y española), la jurisprudencia y la práctica comercial a través de los clausulados ofrece una ex celente experiencia previa para proponer la regulación de esta materia en Guinea-Bissau, pues ya se han detectado los problemas interpretativos, las disfunciones de la práctica y los riesgos. Toda esta experiencia acumulada será muy útil para adaptar el marco normativo, técnico y empresarial a las particulares condiciones sociales, económicas, financieras y jurídicas de Guinea-Bissau.

Universidad Carlos III de Madrid

QUINTO CAPÍTULO

ESTUDIO PROSPECTIVO PARA LA ELABORACIÓN DE UN MODELO TEÓRICO QUE CONTRIBUYA AL DESARROLLO DEL COMERCIO ELECTRÓNICO EN GUINEA-BISSAU

CAPÍTULO: V.

ESTUDIO PROSPECTIVO PARA LA ELABORACIÓN DE UN MODELO TEÓRICO QUE CONTRIBUYA AL DESARROLLO DEL COMERCIO ELECTRÓNICO EN GUINEA-BISSAU

5. Aspectos introductorios

En este capítulo se pretenden identificar, fundamentalmente a través de la matriz DAFO (también conocida como matriz FODA o análisis SWOT en inglés)[641], las fortalezas, debilidades amenazas y oportunidades actuales que presenta Guinea-Bissau para el desarrollo del comercio electrónico. Para la aplicación de dicho método es imprescindible la opinión de los expertos en el tema. Se escogió un grupo lo suficientemente representativo de diferentes organismos: funcionarios de las instituciones bancarias que operan en el país, Ministerio de Ciencia y Tecnología, Ministerio de Justicia y representantes de misiones diplomáticas de Guinea Bissau en el exterior.

El diagnóstico que se quiere realizar deberá ser dinámico y multidimensional para poder caracterizar la naturaleza y el alcance de los retos del país y poseer una visión territorial de todos los problemas que le afectan. El mismo permitirá la jerarquización de estos retos y las orientaciones del país desde una óptica evolutiva y en relación con su posición relativa a escala mundial. El estudio que a continuación se realizará tiene como principal objetivo:

[641] También se puede aplicar la matriz DAFO, a países u organizaciones que no son empresas; Según sostiene ÁLVAREZ SÁNCHEZ, el análisis DAFO es una técnica que "permite analizar la situación de una empresa. Sirve para dar a conocer todas las circunstancias que afectan a una empresa…", en ÁLVAREZ SÁNCHEZ, José Manuel. *La red como soporte de marketing y comunicación.* Vigo: Ideas Propias Editorial, 2005, pp. 117 y ss; las abreviaturas SWOT (Strenghts Weaknesses Opportunities and Threats).

- Determinar la conveniencia de la implementación del comercio electrónico en Guinea-Bissau, valorar su viabilidad, identificar los factores que condicionarán su implantación y proponer un modelo regulatorio.

Objetivos específicos:

- Determinar cuáles son los posibles factores que pueden repercutir negativamente en el desarrollo del comercio electrónico y en los medios de pagos electrónicos en Guinea-Bissau.

- Determinar los factores que repercuten positivamente en la implementación del comercio electrónico y en los medios de pago electrónicos en Guinea-Bissau.

- Presentar acciones que permitan el uso de los medios de pago en Guinea-Bissau.

Antes de comenzar a desarrollar nuestro análisis, para alcanzar los objetivos planteados en los párrafos anteriores creemos que es necesario ofrecer una primera aproximación al país, su situación geográfica y su demografía porque, a pesar de que no son objetivos propios de este capítulo, nos permitirán comprender mejor el alcance de nuestro análisis y el fundamento de nuestras conclusiones.

5.1. Datos generales del país

La República de Guinea-Bissau se encuentra ubicada en la costa occidental de África[642], con una superficie de 36.125 km². Limita al norte con

[642] Vid. FISAS ARMENGOL, Vicenç. *Amílcar Cabral y la independencia de Guinea-Bissau*. Lisboa: Editorial Novas Terra, 1974, p. 15; ALVARENGA, José. «Potencialidades,

Senegal, al este con Guinea Conakry, y al sur y al oeste con el Océano Atlántico[643]. Su territorio está compuesto por una parte continental y otra insular, formada, entre otras, por el archipiélago de Bijagos. El país se divide administrativamente en tres provincias (norte, sur y este), ocho regiones (Bafatá, Biombo, Bolama, Cacheu, Gabu, Oio, Quinara, y Tombali) y un sector autónomo que es la capital (Bissau).

Figura: Mapa de Guinea-Bissau.

Fuente: CIA The World Factbook

política e programas de desenvolvimiento económico em Guinea-Bissau», en *1ªs Jornadas de estudios sobre la cooperación para al desarrollo entre Europa y los países del área Sub-Sahariana, República Popular de Angola, República de Cabo Verde, República de Guinea Bissau, República Popular de Mozambique, Madrid, 28, 29, y 30 de septiembre de 1989*. Madrid*:* Editorial IEPALA, 1989, páginas: 1 carpeta.

[643] FISAS ARMENGOL, Vicenç. *Amílcar Cabral…*op., cit.*,* p. 15.

La parte continental se caracteriza por ser una región costera, de planicies bajas y pantanosas, excepto en la parte oriental, donde algunas extensiones de la meseta de Futa Djalo alcanzan una altura de 300 metros.

A lo largo de la costa abundan los estuarios cenagosos y las rías. Las mareas tienen una importancia decisiva en el sistema hidrográfico y en la economía del país. La amplitud de las mareas alcanza los valores más altos de toda África occidental. La penetración de las mareas en el interior y la existencia de los ríos desempeñan una importancia vital en el sistema de transporte, por permitir en muchos lugares la navegación de los navíos de largo recorrido y también la navegación de l anchas. La zona costera pantanosa es apta para el cultivo de arroz. En el este se practica la agricultura (maní, arroz, palma oleaginosa) y la ganadería. La necesidad de incrementar las exportaciones provoca el uso excesivo de los suelos, mientras las plantaciones de arroz sustituyen parte de los bosques de la costa.

Por otra parte, se ha de resaltar que el país cuenta con grandes reservas de recursos naturales: petróleo[644], bauxita y fosfato, estas dos últimas están en proceso de explotación desde 2010[645].

El clima es tropical húmedo, con temperaturas que oscilan entre los 20º C y los 30º C[646], con una estación seca de noviembre a mayo y una estación lluviosa de mediados de mayo a finales de octubre o principios de

[644] Vid. "Exploração da bauxite em Boé", *Boletim de informação sobre petróleo e minas na Guiné-Bissau*, núm. 0 Outubro de 2011, p. 5.

[645] Esta información fue publicada por CIA [En línea] disponible en Internet: https://www.cia.gov/library/publications/the-world-factbook/geos/pu.html(última consulta, 20 de diciembre de 2012); vid. Contratos firmados entre el gobierno de Angola y de Guinea-Bissau para la explotación de bauxita, ver "L'Angola, nouveau maitre de la filière bauxitique", en *Africa Mining Intelligence*, núm. 238, 17 de novembro de 2010; vid. "Guinea Bissau signs bauxite mining agreement with Angola", *Macau Hub*, 17 de Setembro de 2007.

[646] Vid. *Geografía de Guinea Bissau* [En línea] disponible en Internet: http://www.ikuska.com/Africa/economia/paises.htm (última consulta, 20 de noviembre de 2012).

noviembre. La precipitación anual es de 2.500 mm en la parte sur del país mientras que en la parte norte es de 1400 mm. Los principales hábitats naturales están formados por manglares, bosques de palmeras, bosques secos y semi secos, sabanas húmedas de árboles o de pastizales, bancos de arena y hábitats marinos con un substrato rocoso.

El archipiélago de Bijagós es un área donde coexisten varios ecosistemas caracterizados por la riqueza de su biodiversidad, tanto en sus bosques como en la flora costera. Aproximadamente el 30 % de sus costas están cubiertas de manglares. El archipiélago de Bijagós se encuentra en la confluencia de las corrientes provenientes de Canarias, por el norte, y las provenientes del golfo de Guinea. Particularmente en invierno, las corrientes del norte traen consigo cantidades importantes de nutrientes que favorecen la multiplicación de fitoplancton. Además, los ríos del continente aportan un flujo constante de nutrientes hacia las aguas del archipiélago.

El archipiélago de Bijagós se sitúa a lo largo de la costa de Guinea, en un área de más de 10.000 Km², de los cuales sólo el 10 % es tierra firme. Está compuesto por más de cien islas e isletas, de las que unas veinte están habitadas.

Las islas habitadas del archipiélago de Bijagós son territorio del Pueblo Bijagós, grupo étnico muy diferenciado de Guinea-Bissau. Sus conocimientos para el aprovechamiento de los recursos les han permitido vivir durante siglos sin poner en peligro la reproducción y mantenimiento de los mismos. Por esta razón, desde el principio de creación de la Reserva de la Biosfera han sido parte fundamental en su consolidación.

Finalmente, cabe concluir que, si bien la situación del transporte en el país no es ciertamente muy complicada debido a la relativamente reducida población, es cierto, sin embargo, que es inadecuado. En la parte insular se

concentran las mayores deficiencias en el transporte, ya que el país cuenta con pocos navíos para transportar mercancías y pasajeros a las islas. A nuestro juicio, dicha situación no representa un alto riesgo para el desarrollo del comercio electrónico en el país, sino más bien contribuiría a mejorar dicha situación, en particular, para el desarrollo de la prestación de servicios y el ofrecimiento de bienes intangibles. No obstante, no puede desconocerse el hecho de que afectaría indirectamente al comercio electrónico de bienes tangibles que precisan una red sólida y amplia de servicios logísticos.

A. Demografía y sociedad

El país cuenta con 1. 628.603 habitantes (julio de 2011)[647]. La variedad de etnias constituye la característica más marcada de la población guineana, con múltiples idiomas, costumbres y diferentes estructuras sociales. Casi el 99% de los guineanos son de raza negra y se pueden dividir en las siguientes tres etnias: Fula (20%) y Mandinga (13%), están concentradas en el norte y noreste; Balanta (30%) y Pepel (10%), que viven en las regiones costeras del sur y los Manjaco (14%) y Mancanha (1 %) que ocupan las áreas costeras centrales y del norte. La mayoría de la población restante son mestizos de ascendencia portuguesa y negra, incluyendo una minoría caboverdiana. Los portugueses puros constituyen sólo una porción muy pequeña de los guineanos.

B. Idiomas hablados

El idioma oficial es el portugués, hablado por tan solo el 14% de la población. El 44% de la población habla el creole (kriol) y el resto, idiomas nativos africanos: Badjara, Balanta-Kentohe, Basary Fula, Bayote, Bainoukgunyuno, Biafada (2%), Bijagós (2%), Cassanga, Ejamat, Kobiana,

[647] Dato ofrecido por la Oficina del Censo de EE.UU [En línea] disponible en Internet: http://www.indexmundi.com/es/guinea-bissau/poblacion.html(última consulta 10 de junio de 2011); vid. [En línea] disponible en Internet: https://www.cia.gov/library/publications/the-world-factbook/geos/pu.html (última consulta 20 de noviembre de 2012).

Mancanha, Mandinga, Manjako, Mansonka, Nalu, Pepel y Soninke. Entre las creencias religiosas, el 47% son animistas, el 45% musulmán; y menos del 8% cristiano, la mayoría de ellos católicos.

Debemos hacer notar que el hecho de que se hablen varias idiomas o dialectos en el país no influye negativamente en la implementación de redes de comunicación ya que el 44% de la población habla el idioma criollo (kiriol) que es la lengua más hablada en todo el país, sin excluir el portugués como idioma oficial. Además, existe un porcentaje muy elevado de la población que habla francés e inglés.

Sin embargo, desde el punto de vista de la estabilidad del país, se puede afirmar que las diversidades étnicas existentes (con múltiples idiomas y diferentes estructuras sociales) contribuyen, de una forma u otra, a su inestabilidad política y económica. Desde su independencia de Portugal, el 24 de septiembre de 1973, hasta la actualidad, el país ha sufrido golpes de Estado, intentos de golpes de Estado y asesinatos de líderes políticos y militares[648]; es decir, Guinea-Bissau es un país políticamente inestable[649]

[648] Vid. CAMPO, Americo. História da Guiné-Bissau em datas. Lisboa: 2012, 60 p; ROMERO JUNQUERA, Abel. «La arquitectura de paz y seguridad africana. Un compromiso de la Unión Europea», en La importancia geoestratégica del África subsahariana. Centro Superior de Estudios de la Defensa Nacional (España): Editorial, Ministerio de Defensa, Secretaría General Técnica, 2010, p. 165; CORDEIRO, Roberto Sousa. *Guiné-Bissau 1973-2005: uma relação civil-militar no processo de transição política*. [En línea] Disponible en Internet: http://www.didinho.org/GUINEBISSAUUMAANALISESOBREARELACAOCIVILMILITAR.pdf (última consulta 12 de junio de 2012); Dança de cadeira: Golpes de Estado entre Autoritarismo e a Democracia guineense [En línea] Disponible en Internet: http://www.didinho.org/Dancadecadeira.pdf(última consulta 12 de junio de 2012) 21 p; *Guiné-Bissau:entre as sombras do militarismo e da impunidade*. [En línea] Disponible en Internet: http://www.didinho.org/GUINEBISSAUENTREASSOMBRASDOMILITARISMOEDAIMPUNIDADE.pdf(última consulta 12 de junio de 2012); vid. AUGEL, Johannes; CARDOSO, Carlos. Transição Democrática na Guiné Bissau. Bissau: INEP, 1996; CARDOSO, Carlos (s/d). Os *desafios da transição política na Guiné Bissau*. [En línea] Disponible en Internet: http://www.didinho.org/osdesafiosdatransicaopoliticanaguinebissau.htm(última consulta 12 de junio de 2012); FERREIRA, Mario; NUMERIANO, Roberto. *O que é golpe de Estado*. São Paulo: Brasiliense, 1993, p. 7; Vid. Comisión Europea: *Comunicación de la Comisión al*

Porque, a pesar de que existe un s istema democrático que permite elecciones libres, siguen existiendo conflictos internos entre las fuerzas políticas y los militares[650].

Por último, se ha de d estacar que la mayor parte de la población se localiza en l as zonas rurales y el resto se concentra en la capital. Esta situación no representa ningún obstáculo para la implementación del comercio electrónico en el país, sino que más bien representa una oportunidad pues permitiría el acceso a bienes y servicios de una población dispersa en áreas rurales.

Para ubicar el país en su entorno geográfico, político y social, es preciso analizar a continuación los organismos regionales de integración de los que Guinea-Bissau es miembro. El análisis de este nivel de integración regional del país nos va a ofrecer una variable de oportunidades a la hora de trazar

---

Consejo relativa al inicio de consultas con la República de Guinea-Bissau en aplicación del artículo 96 del Acuerdo de Cotonú revisado. Bruselas, 20 de diciembre de 2 010. COM (2010) 766 final [En línea] disponible en Internet: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0766:FIN:ES:PDF(última consulta 10 de junio de 2012) 34 p; Guiné-Bissau: «Para Lá da Lei das Armas», *Briefing África do Crisis Group* N°61, 25 de Junho de 2009. [En línea] disponible en Internet http://www.crisisgroup.org/fr/regions/afrique/afrique-de-louest/guinee-bissau/B061-guinea-bissau-beyond-rule-of-the-gun.aspx?alt_lang=pt(última consulta 2 de j unio de 201 2); CORDEIRO, Roberto Sousa. *Guiné-Bissau:entre as sombras do militarismo e da impunidade.* [En línea] Disponible en Internet: http://www.didinho.org/GUINEBISSAUENTREASSOMBRASDOMILITARISMOEDAIMPUNIDADE.pdf (última consulta 13 de junio de 2012);

649 «Guinée-Bissau: besoin d'Etat», *Relatório África* do Crisis Group N°142, 2 de Julho de 2008[En línea] disponible en I nternet: http://www.crisisgroup.org/fr/regions/afrique/afrique-de-louest/guinee-bissau/142-guinea-bissau-in-need-of-a-state.aspx(última consulta 2 de junio de 2012).

650 Vid. «Para além dos compromisos: as perspectivas de reforma na G uiné-Bissau», *Relatório África do Crisis Group*, núm. 183. Dakar, 23 de janeiro de 2012, 41 p. [En Línea] disponible en Internet: http://www.crisisgroup.org/fr/regions/afrique/afrique-de-louest/guinee-bissau/183-beyond-compromises-reform-prospects-in-guineabissau.aspx?alt_lang=pt (última consulta 2 de junio de 2012); vid. KOUDAWO, Fafali, MENDY, Peter Karibe. *Pluralismo político na Guiné-Bissau:* uma transição em curso. Bissau: INEP, 1996; TEIXEIRA, Ricardino. *Tiro na democracia: uma análise sobre o processo de transição democrática na Guiné-Bissau, 1994-2007*. [En línea] Disponible en Internet: http://www.didinho.org (última consulta 12 de junio de 2012).

las estrategias de modernización tanto desde una perspectiva económica como jurídica.

5.2. Organizaciones regionales de integración en África Occidental

Guinea-Bissau está inmersa en un proceso de integración regional como miembro de diversas organizaciones regionales que a continuación estudiaremos.

A) La Comunidad Económica de Estados del África Occidental CEDEAO/ ECOWAS

Guinea-Bissau[651] es miembro de la Comunidad Económica de Estados del África Occidental (CEDEAO/ ECOWAS por sus siglas en inglés)[652], fundada el 28 de mayo de 1975 con la firma del Tratado de Lagos[653]. Tiene como objetivo promover la integración económica de los países miembros en todos los ámbitos de la actividad económica, en especial la industria, el transporte, las telecomunicaciones, energía, agricultura, recursos naturales, comercio, finanzas, cultura y cuestiones sociales.

En este sentido, el apartado primero del art.3 del Tratado de constitución de la CEDEAO, establece que la finalidad de la comunidad, "es elevar el nivel de vida de sus pueblos, y mantener y mejorar la estabilidad económica, fomentar las relaciones entre los Estados miembros y contribuir al progreso y el desarrollo del continente africano."

Además, se prevé en el Tratado que estos objetivos deberán alcanzarse a través de la creación de una Unión Económica que comprendería la

[651] La República de Guinea-Bissau ratificó el Tratado en 1975.

[652] Sitio visitado http://www.ecowas.int/ (última consulta el 16 de noviembre de 20 11). http://www.crin.org/espanol/RM/ecowas.asp(última consulta,16 de noviembre de 2011).

[653] *Tratado de la CEDEAO*. [En línea] disponible en Internet: http://www.comm.ecowas.int/sec/fr/docs/traite_revise.pdf(última consulta, 20 de mayo de 2012).

creación de un mercado común, la eliminación, entre los Estados miembros, de los obstáculos a la libre circulación de personas, bienes, servicios y capitales, y el reconocimiento del derecho de residencia y establecimiento.

La CEDEAO está constituido por 15 Estados miembros: Benín, Burkina Faso, Cabo Verde, Costa de Marfil, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Níger, Nigeria, Senegal, Sierra Leona, y Togo[654].

Se estructura de la siguiente forma: la Comisión, la Comunidad del Parlamento, el Tribunal de Justicia de la Comunidad y un Banco para la Inversión y el Desarrollo. A continuación estudiaremos las funciones de cada una de ellas.

La Comisión hace recomendaciones y da consejos. Está compuesta por: la Oficina del Presidente, la Oficina del Vice Presidente, la Oficina del Comisionado de Administración y Finanzas, la Oficina del Comisionado de Agricultura, Medio Ambiente y Recursos Hídricos, la Oficina del Comisionado para el Desarrollo Humano y Género, la Oficina del Comisionado de Infraestructuras, la Oficina del Comisionado para la Política Macroeconómica, la Oficina del Comisionado de Asuntos Políticos, la Paz y la Seguridad, la Oficina del Comisionado de Comercio, Aduanas y Libre Circulación.

El Parlamento de la Comunidad lo compone la Asamblea de los pueblos de la Comunidad cuyos miembros se considera que representan a todos los ciudadanos de África occidental[655]. Está compuesto de un ala política y un ala administrativa.

El Banco de la CEDEAO para la Inversión y el Desarrollo (EBID) está formado por: un Consejo de Ministros, la Oficina del Comisionado de

[654] ROMERO JUNQUERA, Abel. «La arquitectura de…»*op., cit*., p. 182.
[655]http://www.parl.ecowas.int/&usg=ALkJrhjqbcOwTF1Hw1DdA0PM0IjNFOWVuQ(última consulta, 19 de mayo de 2012).

Infraestructuras, la Oficina del Comisionado para la Política Macroeconómica, la Oficina del Comisionado de Asuntos Políticos, la Paz y la Seguridad y la Oficina del Comisionado de Comercio, Aduanas y libre circulación.

Cabe destacar además que la Comisión de la CEDEAO y el Banco para la Inversión y el Desarrollo de la CEDEAO, comúnmente denominado el Fondo, son sus dos principales instituciones encargadas de aplicar políticas, ejecutar programas y llevar a cabo proyectos de desarrollo en los Estados Miembros. Esos proyectos incluyen la construcción de carreteras y telecomunicaciones y el desarrollo de los recursos de energéticos, agrícolas, e hídricos intracomunitarios.

Es importante señalar que los Estados miembros de la CEDEAO[656] ocupan una superficie de 1,5 millones de km², lo que representa el 17% de la superficie total del continente. Los países más extensos son Níger (24,8%) y Malí (24,3%), mientras que Guinea-Bissau representa (0,36%), siendo Cabo Verde (0,1%) el país más pequeño.

Desde el punto de vista de la demográfico, Nigeria es el país más poblado de la región CEDEAO con una población de 134,38 millones (51,5%), seguido por Ghana que tiene una población estimada en 22,56 millones (8,6%). Guinea-Bissau tiene una población de 1.596.677 habitantes (2.5 %) y Cabo Verde es el país con menor población, 520 000 habitantes (0,2%).

Finalmente, cabe destacar que en materia de nuevas tecnologías, el Tratado de la CEDEAO contempla, en los apartados 1 y 2 del art. 27, cuestiones relacionada con la "Ciencia y Tecnología". Así, en el apartado

[656] http://www.reingex.com/CEDEAO-Comunidad-Economica-Estados-Africa-Occidental.asp (última consulta 19 de mayo de 2012); También, la CEDEAO desempeña función de mantener la paz en la región.

primero se establece que “Los Estados miembros: a) fortalecerán la capacidad nacional científica y tecnológica con el fin de llevar a cabo la transformación socioeconómica necesaria para mejorar la calidad de vida de la población; b) garantizar la correcta aplicación de la ciencia y la tecnología para el desarrollo(…); d) cooperar en el desarrollo, adquisición y difusión de tecnologías apropiadas, y e) fortalecer las instituciones de investigación científica y tomar todas las medidas necesarias para preparar y ejecutar conjuntos de investigación científica y desarrollo tecnológico”.

Y a continuación el apartado segundo del art. 27 establece que los Estados miembros deberán:

a) armonizar, a nivel comunitario, las políticas nacionales en la investigación científica y tecnológica con el fin de facilitar su integración en los planes nacionales de desarrollo económico y social

b) co-coordinar sus programas de investigación aplicada, investigación para el desarrollo, servicios científicos y tecnológicos

c) armonizar sus planes nacionales de desarrollo tecnológico, con especial énfasis en las tecnologías autóctonas y adaptadas, así como sus reglamentos sobre la propiedad industrial y transferencia de tecnología; (…)

d) llevar a cabo un intercambio permanente de información y documentación de datos y establecer redes comunitarias y bancos de datos

Como hemos señalado a lo largo de este sub-epígrafe, el objetivo trazado en el Tratado de constitución de la CEDEAO es promover la

cooperación y la integración, que permitirán el establecimiento de una unión económica. Sin embargo, desde la firma del Tratado, revisado en 1993, cada vez más la comunidad se ha i do desmarcando de estos objetivos, centrándose más en los asuntos políticos, en el mantenimiento de la paz y la seguridad en l os países miembros. En los últimos años, la CEDEAO ha intervenido en muchos conflictos internos de los países miembros[657], por ejemplo en Guinea-Bissau[658], Guinea Conakry, Sierra Leona, Liberia, Togo y Costa de Marfil.

La región CEDEAO es la comunidad económica regional africana más poblada, por lo que creemos que dicha situación demográfica favorece la implementación del comercio electrónico en la zona.

Por último, cabe concluir que en l a CEDEAO no ex iste ninguna normativa, principios o dec laraciones comunes en materia de l as nuevas tecnologías o comercio electrónico.

B. La Unión Económica y Monetaria del África occidental (UEMOA)

El 2 d e mayo de 1997, Guinea-Bissau se convierte en el octavo país miembro de la Unión Económica y Monetaria del África occidental (UEMOA) y el primero no francófono. La UEMOA fue creada el 10 de febrero de 1994[659] en Dakar (Senegal) por los Jefes de Estados de ochos países de

[657] Vid. ROMERO JUNQUERA, Abel. «La arquitectura de...»*op., cit.,* p. 204; KABUNDA BADI, Mbuyi. «Relaciones internacionales africanas y relaciones interafricanas en la era de la globalización», en ECHART MUÑOZ, Enara (coord.). *África en el horizonte. Introducción a la realidad socioeconómica del África subsahariana*. Madrid: Catarata, 2006, pp. 82 y ss.

[658] Tras el golpe de Estado producido por el llamado Comando militar en Guinea-Bissau, el 12 de abril de 2012, el CEDEAO tuvo que mediar en la liberación del Presidente Interino y el Primer Ministro, ambos detenidos en Amura (la base militar de Bissau). Después de varias reuniones con el Comando Militar, CEDEAO reconoce a los golpistas guineanos, y les piden para formar un gob ierno de transición, y permitir el envío de fuerzas de intervención de los países miembros de la CEDEAO. Reconocimiento que demuestra claramente el interés de los países miembros de CEDEAO en apoderarse de l os yacimientos de Guinea-Bissau.

[659] Tratado de la Unión Económica y Monetaria del África Occidental (UEMAO)
El tratado entró en vigor el 1 de agosto de 1994.

África occidental: Benín, Burkina Faso, Costa de Marfil, Guinea Bissau, Malí, Níger, Senegal y Togo.

Se trata de una unión aduanera y monetaria entre dichos Estados miembros que comparten el uso de una moneda común, el franco CFA[660]. Sus principales objetivos son promover:

- ✓ la mayor competitividad económica, a través de m ercados abiertos, junto a la racionalización y armonización de los entornos legales
- ✓ la convergencia de políticas e indicadores macroeconómicos
- ✓ la creación de un mercado común, la coordinación de políticas sectoriales
- ✓ la armonización de políticas fiscales.

Dicho organismo reúne países con una extensión de 3.509.600 km² y una población de 80.340.000. La tasa de crecimiento es del 3%. El PIB nominal es de 24.332,6 mil millones de FCFA, mientras que el PIB real (a precios constantes) es de 18 .458,8 mil millones de FCFA, la tasa de crecimiento del PIB real es del 4,3% y la inflación anual del 4,3%.

A la vista de todo lo expuesto podemos concluir que la UEMOA se encarga de definir la ley bancaria aplicable a los bancos y a l os establecimientos financieros de los países miembros. El consejo de Ministros de la UEMOA aprueba la Directiva 08/2002/CM/UEMOA[661], de 19 de

http://www.wipo.int/wipolex/es/other_treaties/details.jsp?group_id=24&treaty_id=313(última consulta 14 de mayo de 2012).

[660] El franco CFA es una moneda heredada del pasado colonial y que representa, como pocas otras cosas, el enorme poder que Francia sigue detentando en sus ex colonias. Es la moneda común de nada menos que catorce países, casi todos ex colonias francesas (Costa de Marfil, Senegal, Malí, Níger, Benín, Burkina Faso, Togo, Camerún, Chad, Gabón, República Centroafricana y República del Congo) excepto Guinea Bissau y Guinea Ecuatorial. Emitidos por BCEAO y el Banco de Estados de África Central (BEAC)

[661] UEMOA: Directiva 08/2002/CM/UEMOA, sobre las medidas para promover la banca y el uso de medios de pa go sin dinero en efectivo [En línea] disponible en Internet:

septiembre 2002, que tiene por objeto promover el uso de servicios bancarios y nuevos instrumentos de pago (art. 2 de la Directiva). Del mismo modo, se espera por parte de los Estados miembros de la UEMOA la adopción de leyes similares en consonancia con esta Directiva.

Por su parte, el Reglamento Nº15/2002/CM/UEMOA[662], de sistema de pago en los Estados miembro de la Unión Económica Monetaria del África Occidental (RSPCM), aborda cuestiones relacionadas con la firma electrónica, certificado electrónico, cheque y letra de cambio. Además, en su capítulo I Sección I, prevé lo relativo a las obligaciones de las partes en la transferencia electrónica de fondos. También, en su capítulo II, sección I, se abordan cuestiones relacionadas con la prevención del fraude, el abuso y la falsificación de tarjeta bancaria, instrumentos y métodos de pago electrónico.

En relación con la transferencia electrónica de fondos, el legislador de la Comunidad Monetaria establece en el art. 134 del RSPCM, que al remitente de la orden de pago le corresponde la obligación de garantizar la seguridad de los datos transmitidos en el momento de la emisión de la orden de pago. En especial, adoptar todas las precauciones necesarias de la seguridad técnica de los datos transmitidos. Además, señala que si los datos son obtenidos y utilizados para efectuar un pago en nombre de un tercero seguirá siendo responsable del pago.

El art. 136 del RSPCM prevé que, las relaciones entre el emisor de la tarjeta o de otro instrumento de pago electrónico y el beneficiario son regidas por el convenio de las partes.

---

http://www.bceao.int/Directive_n08_2002_CM_UEMOA.html(última consulta 24 de mayo de 2012).

[662] UEMOA. *Reglamento Nº15/2002/CM/UEMOA, de sistema de pago de 19 de septiembre 2002* [En línea] disponible en Internet: http://www.bceao.int/IMG/pdf/Reglement_n_15_2002_CM_UEMOA_relatifaux_systemesde_paiement_dans_les_Etats_membres_de_l_UEMOA.pdf(última consulta 24 de mayo de 2012). El presente Reglamento tiene por objeto establecer un marco jurídico sobre los sistemas de pago en los Estados miembros de la UEMOA.

En relación con la obligación de informar, el art. 137 del RSPCM establece que los organismos mencionados en el artículo 42 de este Reglamento están obligados a informar, a cualquier persona que así lo solicite, sobre las condiciones de uso de tarjetas bancarias, instrumentos y procesos de pagos electrónicos que se emiten, y las sanciones por el mal uso.

Por su parte, el art. 140 del RSPCM prevé que en caso de utilización abusiva, en los cuatro (4) días hábiles que siguen la comprobación de esta utilización, el establecimiento emisor deberá ordenar al titular de restituir su tarjeta e informar sobre esta decisión al Banco Central, que tiene un fichero que censa las decisiones de retirar las tarjetas.

En la Sección 2 del Capítulo II del RSPCM, se estipula lo relacionado con *la reprimenda de los fraudes, los abusos y las falsificaciones.* En este sentido, el art. 143 RSPCM establece que serán castigados por penas previstas en el precepto 84 de la ley uniforme sobre los instrumentos de pago. Los que fraudulentamente se hayan apropiado de una tarjeta bancaria u otro instrumento electrónico de pago; los que hayan suplantado o falsificado una tarjeta bancaria u otro instrumento electrónico de pago; los que, en conocimiento de causa, hayan hecho uso o intentado hacer uso de una tarjeta bancaria u otro instrumento electrónico de pago, falsificado u obtenido fraudulentamente.

Los que, con conocimiento de causa, hayan aceptado recibir un pago por medio de una tarjeta bancaria o por medio de otro instrumento electrónico de pago imitado, falsificado u obtenido de modo fraudulento; los que hayan detenido, con conocimiento de causa, una tarjeta bancaria u otro instrumento electrónico de pago falsificado o fraudulentamente.

Por último, cabe destacar que existe Instrucción nº 01 / 2006 / SP, de 31 Julio 2006 relativa a la emisión del dinero electrónico y las entidades de dinero electrónico[663].

C) Organización Africana de Armonización del Derecho Mercantil (OHADA, según sus siglas en francés)

También es importante destacar que Guinea-Bissau es miembro de la Organización Africana de Armonización del Derecho de los Negocios (OHADA)[664], creada por el Tratado firmado en Port Louis, Islas Mauricio, el 17 de octubre de 1993. Dicha organización está integrada por países de la Unión Económica y Monetaria del África Occidental (UEMOA)[665], de la Comunidad Económica y Monetaria del África Central (CEMAC)[666], las Comoras y Guinea.

El Tratado de la OHADA y sus diferentes actos uniformes tienen por objetivo principal remediar, disminuir o atenuar la inseguridad jurídica de las actividades económicas en los Estados miembros mediante la adopción de textos jurídicos comunes, de aplicación directa en los Estados miembros y mediante la aplicación de procedimientos judiciales apropiados.[667] Las instituciones que conforman la OHADA son:

---

[663] [En línea] disponible en Internet: http://www.bceao.int/IMG/pdf/INSTRUCTION_N_o_01_-_2006_-_SP_DU_31_JUILLET_2006.pdf (última consulta, 25 de noviembre de 2012).

[664] Guinea-Bissau firma el Tratado de adhesión de la OHADA mediante la Resolución nº 1/94 del Consejo de Estado, publicado en *Boletín Oficial,* núm. 3. Suplemento, de 17 de Janeiro de 1994.

[665] Países miembros de UEMOA que conforman la OHADA (Benín, Burkina Faso, Costa de Marfil, Guinea Bissau, Malí, Níger, Senegal y Togo).

[666] Países miembros CEMAC que conforman la OHADA (Camerún, Chad, Gabón, República Centroafricana, Congo, y Guinea Ecuatorial).

[667] Los "actos uniformes" son textos legislativos aprobados por los países miembros de la OHADA y con fuerza de ley; son aplicables en los diferentes países miembros ("Actas Uniformes OHADA". [En línea] disponible en Internet: http://www.ohada.com/textes.php?categorie=38(última consulta el 18 de noviembre de 2012).

- El Consejo de Ministros, que es el órgano de decisión, encargado de adoptar las actas uniformes[668]

- El Tribunal Común de Justicia y de Arbitraje[669] que es el órgano judicial que tiene como función asegurar a los Estados miembros, la interpretación y la aplicación del Tratado, así como de sus actas uniformes

- La Secretaría Permanente, institución que asiste al Consejo de Ministros y que tiene como función específica preparar proyectos de actas uniformes (en concertación con los gobiernos de los Estados miembro)[670], y además ejerce la tutela sobre la Escuela Regional Superior de Magistratura

- La Escuela Regional Superior de Magistratura que tiene como función asegurar la formación de magistrados y de auxiliares de justicia de los Estados miembro de la OHADA.

Por último, se ha de concluir que hasta el momento la OHADA ha aprobado las siguientes normas jurídicas que son aplicables en los 16 países miembros:

[668] Según se prevé en el art. 27 del Tratado de la OHADA, "el Consejo de Ministros estará compuesto por los Ministros encargados de la Justicia y por los Ministros encargados de Hacienda". [En línea] disponible en Internet: http://www.jurisint.org/ohada/text/text.01.sp.html (última consulta el 18 de noviembre de 2012).

[669] Por su parte, el art. 31 del Tratado de la OHADA establece que "el Tribunal Común de Justicia y de Arbitraje estará compuesto por siete jueces, los cuales serán elegidos entre los nacionales de los Estados partes por un periodo de siete año renovable una vez, a fin de desempeñar las funciones y en las condiciones siguientes: 1) magistrados que dispongan de una experiencia judicial de quince años como mínimo y hayan ejercido altas funciones jurisdiccionales; 2) abogados inscritos en el Colegio de Abogados de alguno de los Estados partes, y que dispongan de un mínimo de quince años de experiencia profesional; y 3) profesores de derecho que dispongan de una experiencia profesional mínima de quince años. (…)"

[670] Vid. El art. 6 del Tratado de la OHADA

a) Ley Uniforme sobre Derecho comercial General[671]

b) Ley Uniforme sobre Derecho de Sociedades

c) Ley Uniforme sobre garantías y fianzas

d) Ley Uniforme sobre cobro de deudas y embargos

e) Ley Uniforme de quiebras

f) Ley Uniforme sobre la ley de arbitraje

g) Ley Uniforme contable

h) Ley Uniforme laboral

i) Ley de s obre contratos de transporte de mercancías por carretera

Estos actos uniformes son considerados textos legales supranacionales de obligado cumplimiento en los países miembros de la OHADA. De modo aclaratorio, el legislador de la OHADA señala que las normativas nacionales seguirán siendo aplicables, siempre y cuando no contravengan aquellos.

Entre las normativas mencionadas a lo largo de este epígrafe, sólo el Acta uniforme relativo al derecho comercial general hace referencia al pago del precio en su Título III, Capítulo II, Sección 1.

Según establece el art.233 de la Ley uniforme sobre derecho general comercial de la OHADA[672], el comprador se compromete en las condiciones estipuladas en el contrato y de c onformidad con las disposiciones del presente título a pagar el precio y recibir la mercancía.

[671] J. OHADA, núm. 1 de octubre de 1997, Cotonou

[672] Ley uniforme sobre derecho general comercial de la OHADA [En línea] disponible en Internet:http://www.fdbissau.org/PDF_files/OHADA-COMERCIALGERAL-VERSAO_FINAL.pdf (última consulta, 25 de noviembre de 2012).

Por su parte, el art. 234 de la Ley uniforme sobre derecho general comercial de la OHADA[673], establece que, la obligación de pagar el precio comprende la de adoptar todas las medidas y cumplir con todas las formalidades destinadas a permitir el pago de precio, previstas en el contrato o en las leyes y reglamentos. En este sentido, por ahora no existen normativas sobre comercio electrónico en el seno de la OHADA.

5.3. Situación del sistema bancario en Guinea-Bissau

La subida en la tasa de bancarización registrada en Guinea-Bissau durante la campaña de comunicación y promoción de la bancarización y utilización de los medios de pago utilizados en el espacio de la UEMOA[674] ha sido de un 0,2 por ciento.

Según resalta el Director del Banco Central de los Estados de África Occidental (BCEAO) en Guinea-Bissau en una entrevista[675], "ahora la tasa salió de los 3,2 por ciento para situarse en 3,4 de los 1,5 millones de guineanos, pero aún así el país se sitúa en la cola de la tabla de los países de la UEMOA en términos del nivel de bancarización". Y a continuación reconoce, "…que fue un pequeño pero significativo movimiento para el alta en términos de tasa de bancarización de las poblaciones de Guinea-Bissau".

Para el máximo representante de BCEAO en el país, "a los guineanos les gusta guardar dinero bajo el cojín en vez de encaminarlo para los bancos, y que este tipo de práctica constituye un riesgo, por ejemplo en el

[673] Ibídem,

[674] Entrevista realizada por MENDONÇA, José Augusto*. La tasa de bancarización en Guinea-Bissau sube un 0,2% en seis meses.* [En línea] disponible en Internet:http://www.agareso.org/es/actualidad/mundo/guinea-bissau-cronicas-de-baba/item/443-a-taxa-de-bancarización-en-guinea-bissau-sube-un-02-en-seis-meses(última consulta 3 de noviembre de 2012).

[675] BCEAO es el instrumento financiero de los ocho Estados miembros de la Unión Monetaria del África Occidental. Es una institución pública internacional cuya sede se encuentra en Dakar.

caso de un incendio". Al mismo tiempo, sostiene que "el ahorro de las familias, en vez de quedar guardado en casa, donde corre el riesgo de ser destruido por el fuego, debe ser encaminado hacia los bancos de forma a incrementar la capacidad de estos en conceder créditos, que poseen un efecto de "palanca en la economía"[676].

Respecto a la tesis sostenida por el alto representante de BCEAO en el párrafo anterior, opinamos que no son correctas dichas afirmaciones pues el problema está en que desde los tiempos de los colonos portugueses nunca existió una cultura bancaria que tampoco llegó a nacer después de la independencia. A pesar de que en la década de los 90 el país contaba con el Banco Internacional de Guinea-Bissau (BIGB), lo cierto es que duró poco, tras la aparición de muchas irregularidades por parte de quienes venían beneficiándose de los servicios que esta entidad ofrecía.

Se ha de reiterar que la escasez de ahorro constituye una traba para la bancarización en el país y para la canalización del ahorro a la inversión. Por lo tanto, si no se invierte en crear empresas y puestos de trabajo, la productividad de la economía guineana no puede mejorar y no pueden aumentar los ingresos.

En este sentido, el bajo nivel de bancarización en el país se debe principalmente el bajo nivel de ingresos promedio por la población. Por lo que las tesis sostenidas por el director del BCEAO, en algunos puntos, son inaceptables. Es decir, sólo en la medida en que el país crezca y se desarrolle económicamente, se abrirán enormes posibilidades para un mayor nivel de bancarización y consumo. Además, la consolidación de la confianza bancaria aumentaría el nivel de bancarización en el país.

[676] MENDONÇA, J. A. *La tasa…op., cit.,* p. 2

El sistema bancario de Guinea-Bissau es subdesarrollado, el país carece de un Banco Central nacional que trace las políticas monetarias, ya que con su adhesión a la Unión Económica y Monetaria de África Occidental, el 5 de marzo de 1997, el artículo 5 de la Ley 1/97 de 19 de marzo de 1997[677], pone fin a la existencia del Banco Central de Guinea-Bissau, tras establecer que dicha entidad cesa en todas sus funciones, actividades, nombramientos, servicio de emisión de notas y monedas que son transferidos al Banco Central de los Estados de África Occidental (BCEAO).

Aproximadamente el 90% de la población vive en áreas rurales donde no hay servicio bancario. Muy poca población tiene cuenta bancaria lo que demuestra que la gran parte de las transacciones son efectuadas en dinero en efectivo. Los pagos efectuados por otros medios son poco frecuentes y están poco desarrollados.

Los servicios de pago son básicamente manuales y los instrumentos de pago tales como las transacciones electrónicas de fondos o las tarjetas de crédito como medios de pagos en el comercio electrónico, todavía no han sido introducidas. Los servicios de cajeros automáticos son actualmente ofrecidos solamente por algunos bancos comerciales en algunas de sus sucursales.

Actualmente en los países desarrollados, las nuevas tecnologías de la información han incidido positivamente en todas las actividades económicas y, en particular, en la actividad del banco y de su sistema vital que es el sistema de pagos cuyo desarrollo ha sido inducido por la innovación tecnológica asociada al desarrollo de la informática y de las telecomunicaciones.

[677] Guinea-Bissau: Ley 1/97, de 19 de marzo de 1997, en *Suplemento del Boletín oficial* núm. 12, de 24 de marzo de 1997, Bissau.

Para llevar adelante con éxito la creación de un sistema de pago electrónico en Guinea-Bissau y facilitar así, paralelamente, el desarrollo del comercio electrónico, es imprescindible garantizar la seguridad jurídica, lo que no constituye tarea fácil ya que se trata de una materia en constante mutación aunque sólo sea por la fuerza de la evolución tecnológica de las telecomunicaciones que requiere el dinamismo que caracteriza el comercio electrónico.

Por último, se ha de señalar que los medios de pagos existentes en el país son: cheques, transferencias de fondo y tarjetas de débito.

5.4. El pago a través de dispositivo móvil en Internet en África

Siguiendo el criterio sostenido por algunos autores, "el teléfono móvil ha ido adquiriendo progresivamente la funcionalidad de otros aparatos de uso habitual, como el ordenador de mano, la agenda personal o incluso la grabadora de vídeo"[678]. En la actualidad las entidades bancarias y las operadoras de telefonía móvil se han implicado en el desarrollo de plataformas que permitan gestionar los pagos a través de dispositivo móvil.

El teléfono móvil es un instrumento de comunicación imprescindible en la sociedad, debido a su progresiva sofisticación tecnológica, lo hace que cada vez más pueda considerarse como un medio ideal para la realización de transacciones[679].

Para algunos autores[680], "el progresivo aumento del, número de usuarios del teléfono móvil convierte este instrumento en un medio ideal para ser utilizado como monedero para efectuar pagos, especialmente de pequeñas

[678] JESÚS MILLAN, Ramón. *El pago por móvil empieza a desplegar.* [En línea] disponible en Internet: http://www.networkworld.es/El-pago-por-movil-empieza-a-despegar/seccion-analisis/articulo-151153 (última consulta el 11 de noviembre de 2012).
[679] LIBRERO, Eduardo (coord.). *El libro del…*op., cit., p. 313.
[680] LAFUENTE SÁNCHEZ, R. *Los servicios*…op., cit., 316 y ss.

cuantía, (…). Además, este mismo autor destaca que estamos ante una forma de dinero electrónico, por cuando las tarjetas prepagadas de teléfonos móviles encajan dentro del concepto de "instrumentos de dinero electrónico recargables en forma de tarjetas" "

En la actualidad existen dos modalidades de medios de pagos a través de dispositivo móvil: el pago en el comercio móvil (m-comerce)[681] y el pago a través de dispositivo móvil en Internet. Entre estas modalidades, estudiaremos ésta última, el pago a través de dispositivo móvil en el comercio electrónico, especialmente en Internet, que es más afín a nuestro estudio.

La operativa de pago a través de dispositivo móvil consiste en asociar a un dispositivo móvil una o varias tarjetas de crédito o débito emitidas por una entidad bancaria o financiera. El dispositivo móvil puede ser utilizado para pagar, las compras realizadas en Internet, en los establecimientos comerciales, entre otras. Además, se puede utilizar para consultar los saldos y movimientos de cuenta tal como se hace en un cajero automático[682].

En comparación con otros medios de pago electrónico (tarjeta de crédito o débito), el pago a través de dispositivo móvil permite la reducción de costes para los usuarios y proveedores de bienes o servicios; es decir, las comisiones que las entidades bancarias les aplican por el uso de tarjeta de crédito o débito en el comercio electrónico, así como en las transacciones presenciales, duplican a las que les aplican a las plataformas de pago por

[681] El pago en el comercio móvil se lleva a cabo cuando los usuarios de la telefonía móvil pretenden adquirir o descargar los polífonos, videos, juegos, ver televisión directamente de su móvil, entre otros servicios que se ofrecen; vid., LAFUENTE, SÁNCHEZ, R. *Los servicios…*op., cit., pp. 317 y ss. según señala este autor, el comercio móvil es el conjunto de transacciones económicas efectuadas a través de una red de telecomunicaciones inalámbrica, o sea, una red telefónica.

[682] Según pone de manifiesto ADICAE, que "el conjunto de la tarjetas asociadas, está directamente vinculada a un SIM del teléfono móvil y que únicamente se activara con el PIN del medio de pago con el que se desea operar"; vid. LIBRERO, E. (coord.). *El libro del…*op., cit., p. 313.

móvil. Sin embargo, existen riesgos en el uso del móvil como medio de pago en Internet.

1. *La utilidad del dispositivo móvil en África*[683]

El acceso de los servicios bancarios en África es muy limitado, por lo que el porcentaje de bancarización es muy bajo, situación que obstaculiza el desarrollo socio-económico en la región. No obstante, en los últimos años, el pago mediante dispositivo móvil se ha convertido en uno de los principales motores de la bancarización de la población en ciertos países de África, por ejemplo, Kenia y Sudáfrica, que aprovechan la penetración de los dispositivos móvil en sus territorios para utilizarlos como medio de pago. El uso masivo de este medio de pago en estos países ha permitido que el número de usuarios de telefonía móvil exceda al número de usuarios con cuentas bancarias[684].

Por otra parte, cabe señalar que después del continente asiático, África es el segundo mercado de la telefonía móvil más grande del mundo. Entre los países con mayor crecimiento en África destacan Nigeria[685], Sudáfrica[686] y Kenia[687].

[683] Vid. SÁNCHEZ NAVARRO, Eulogio. *«África subsahariana. Sus recursos y desarrollo», en La importancia geoestratégica del África subsahariana.* Centro Superior de Estudios de la Defensa Nacional (España): Editorial, Ministerio de Defensa, Secretaría General Técnica, 2010 p. 265

[684] JAVIER, Santomas y PRIOR, Francese. *La banca móvil como catalizador de la bancarización de los pobres: modelos de negocio y desafíos regulatorios.* [En línea] disponible en Internet: http://www.redmicrofinanzas.cl/web/wp-content/uploads/2010/07/La-Banca-M%C3%B3vilcomo-catalizadora-de-la-bancarizaci%C3%B3n-de-lospobres.pdf(última consulta el 21 de noviembre de 2012).

[685] Nigeria: la nación más poblada de África, y es el país con mayor número de teléfonos móviles (93 millones de suscriptores), lo que supone un 16 por ciento del volumen total del continente.

[686] En relación a los servicios de banda ancha e Internet móvil, Sudáfrica es el mercado más desarrollado, con un 6 por ciento de penetración, seguido de Marruecos, con un 2,8 por ciento.

[687] *M-Pesa* es un sistema creado por la operadora de teléfono móvil *Safaricom* en Kenia, que permite a los usuarios realizar traspasos de dinero electrónico, lo que supone una

Según el informe publicado por la Asociación Internacional de Operadores de Telefonía Móvil (GSMA, por sus siglas en inglés), durante el segundo cuatrimestre de 2011 se llegó a 649 millones de conexiones en el continente africano, después de haber superado el 50 por ciento de penetración durante 2010[688]. Se espera que se alcancen en África los 735 millones de usuarios a finales del 2012.

2. *Componentes de seguridad exigidos en el pago mediante teléfono móvil*

Hemos de reiterar que, al igual que la seguridad en los pagos mediante tarjeta de crédito en el comercio electrónico, la seguridad en el pago a través de terminales móviles constituye un aspecto clave[689], con independencia de la tecnología utilizada. Por lo que cabe destacar que un sistema seguro de pago por móvil deberá reunir los mismos requisitos o componentes de seguridad que se exigen para garantizar una transacción segura en:

a) confidencialidad.
b) integridad, con la finalidad de impedir que ni la información ni los sistemas sean vulnerados por terceras personas.
c) disponibilidad.
d) autentificación, para evitar el uso no autorizado.
e) autorización, verificación de que el usuario está autorizado para hacer la transacción solicitada.

---

auténtica revolución en un país con limitada infraestructura financiera. Quien inicia el pago suele ser un particular, y quien lo recibe puede ser otro particular, un comerciante con una cuenta ordinaria (y que, por tanto, es un usuario más de la red) o un comerciante con una cuenta de empresa. En cualquier caso, y al tratarse de un sistema cerrado, Safaricom realiza el procesamiento de la operación sin recurrir a esquemas preexistentes; por otra parte, cabe destacar que Kenia lidera la lista de países africanos en servicios de banca móvil y transferencias, con un total de 8,5 millones de usuarios.

[688] WRITER, Staff. *África ya es el segundo mayor mercado de móviles.* [En línea] disponible en Internet: http://www.afrol.com/es/articulos/37755(última consulta 23 de junio de 2012).

[689] Vid, FERNÁNDEZ GÓMES, E. *Conocimientos y aplicaciones*…op., cit., pp. 242-243.

f) no-repudio.

3. Mecanismos de autenticación de las compras y el pago

- *Protocolo USSD (Unstructures Supplementary Services)*[690]*.* Es utilizado por Mobipay y consiste en la utilización de mensajes cortos de texto. Este protocolo forma parte del estándar GSM (Global System for Mobile Communications), basado en secciones transaccionales; es decir, a diferencia del SMS que permite efectuar diferentes operaciones en tiempo real evitando así los retrasos por almacenamiento y reenvío del mensaje, y que no se corta hasta que finalice el proceso, evitando así el riesgo de pérdidas o duplicidades. Este tipo de protocolo o mecanismo puede ser utilizado en zonas donde hay una mínima cobertura, donde es difícil enviar SMS o en lugares donde no se pueden realizar llamadas, por ejemplo en las zonas rurales.

- *Otros mecanismos o protocolos para autenticar las compras y el pago*[691]*.* Son aquellos que consisten en el envío de llamadas de voz automatizadas para autorizar la transacción y en mensajes cortos de textos SMS para confirmarla. Son mecanismos utilizados por Paybox y CaixaMovil.

Por último, para solventar algunos inconvenientes que presentaban las dos primeras generaciones de móvil, surge la UTMS (*Universal Movil Teleccomunication System)* diseñado para funcionar en todo el mundo, que emplea redes terrestres, inalámbricas y enlaces por satélite, lo que le otorga

[690] JESÚS MILLÁN, Ramón. «El pago por móvil empieza a despegar», en *Comunicaciones Word*, núm. 181, 2003.
[691] *Ibídem*

gran movilidad. El cambio de red (*roaming)* es instantáneo, sin cortes en la comunicación.

4. *Situación actual de la telefonía móvil en Guinea-Bissau*

Es necesario abordar en este epígrafe la situación actual de la telefonía móvil en Guinea-Bissau. Según los datos publicados por la Unión Internacional de Telecomunicaciones, el sector de la telefonía móvil en Guinea-Bissau experimentó un fuerte crecimiento, pasando de 1.275,00 abonados en 2003 a 594.100, 00 en 2010[692]. Además, la tasa de penetración se ha elevado del 0.10 % en 2003 al 39.21% en 2010. En este sentido, en comparación con los datos de penetración de Internet en Guinea-Bissau, que hemos mencionado en uno de los epígrafes de este capítulo, cabe resaltar que la telefonía móvil crece más rápido que cualquier otra tecnología de la información y las comunicaciones en nuestro país.

El mercado de la telefonía móvil en nuestro país está marcado por la presencia de tres operadoras que destacan por su presencia en la región: la senegalesa SONATEL (que comercializa la marca Orange Bissau), MTN y Guinetel. Por último, cabe resaltar que el mercado guineano de telefonía móvil está centrado en los servicios de voz, datos (SMS) e Internet.

Finalmente, el uso del teléfono móvil como medio de pago alternativo a la tarjeta de crédito en el comercio electrónico puede contribuir positivamente a la bancarización de la población en Guinea-Bissau ya que permite llegar a zonas rurales donde no existen servicios bancarios ni están conectadas por infraestructuras de telecomunicación. Es el gran motor que

[692] Datos sobre Guinea-Bissau. [En línea] disponible en Internet: http://www.indexmundi.com/facts/indicators/IT.CEL.SETS/compare?country=gw(última consulta 8 de junio de 2012). Por otra parte, cabe resaltar que estos datos representan las suscripciones a un servicio público de telefonía móvil utilizando tecnología celular, que proporciona acceso a la red telefónica pública.

puede jugar un rol fundamental en la bancarización de la población guineana[693].

Por ello, las entidades bancarias guineanas deben aprovechar la penetración de la telefonía móvil para aumentar la tasa de bancarización.

5.5. La situación actual del derecho guineano frente al comercio electrónico

En este epígrafe se pretende analizar brevemente la actual situación del marco jurídico en Guinea-Bissau frente a las nuevas tecnologías y proponer algunas modificaciones. Creemos imprescindible aportar algunos datos y reflexiones acerca del estado en que se encuentra el derecho guineano frente al comercio electrónico.

Como se ha señalado con anterioridad en uno de los epígrafes de este capítulo, Guinea-Bissau es uno de los países más pequeños del continente africano en el que la mayor parte de la población carece de acceso a Internet. Además, el país carece de capital humano preparado para hacer frente a los desafíos que plantea el comercio electrónico.

Por otro lado, cabe destacar que en el ordenamiento jurídico guineano se da la separación entre el Derecho Civil y el Derecho Mercantil, denominado aquí Derecho Comercial, que es la terminología utilizada en los países de habla portuguesa. Por otra parte, se ha de reseñar que existe el Código Civil[694] y la Ley de Procedimiento Civil (Código de Proceso Civil)[695] para dirimir los pleitos civiles.

[693] El pago mediante el teléfono móvil en nuestro país puede fomentar el uso de la tarjeta de crédito, ya que permite la autenticación del usuario.

[694] GUINEA-BISSAU: *Código civil e legislaciones complementaria*. [En línea] disponible en Internet: http://www.fdbissau.org/html_files/legislacao.html (última consulta, 14 de mayo de 2012).

Sin embargo, no existe una normativa nacional sobre comercio. No existe un Código de Comercio a nivel nacional, aplicándose la Ley Uniforme sobre Derecho Mercantil General (acto uniforme relativo al derecho comercial general) que es de obligatorio cumplimiento en todos los países miembros de la OHADA[696].

En Guinea-Bissau las materias relacionadas con las nuevas tecnologías de la información y la comunicación, así como la protección del consumidor en el comercio electrónico, no están reguladas ni en la Constitución[697]ni en el Código Civil ni en el Código Penal[698]. Por ello, en este epígrafe se plantea la necesidad de llevar a cabo una reforma profunda del marco jurídico que supondría una oportunidad además para introducir disposiciones que puedan ir componiendo un derecho de los consumidores y usuarios guineanos ante los problemas que puedan derivar del uso de los medios de pago electrónicos en el comercio electrónico, especialmente en Internet.

Conviene recordar que la Constitución guineana no recoge explícitamente en su texto el derecho a la intimidad, menos aún la libertad informática o su garantía. En este sentido, creemos fundamental hacer una reforma de la carta magna, con la intención de incluir preceptos o incisos sobre el uso de la informática y otras técnicas y medios de tratamientos automatizados de

[695] GUINEA-BISSAU: Código del Proceso Civil y Legislación Complementaria*,* en *Boletín Oficial,* núm. 41, de 13 de octubre de 1993, 323 p. [En línea] disponible en Interne: http://www.fdbissau.org/html_files/legislacao.html (última consulta, 14 de mayo de 2012).

[696] OHADA: *Ley Uniforme sobre Derecho Mercantil General (Acto uniforme relativo al derecho comercial general)* [En línea] disponible en Internet: http://www.fdbissau.org/PDF_files/OHADA-COMERCIALGERALVERSAO_FINAL.pdf (última consulta 20 de mayo de 2012).

[697] Guinea-Bissau: La Constitución de la Republica de Guinea-Bissau, probada el 16 de mayo de 1984(modificada en 1996, por la Ley Constitucional nº 1/96, publicada en *Boletín Oficial* núm. 50, de 16 de diciembre de 1996).

[698] Guinea-Bissau: Código Penal (Decreto-Ley 4/93 – *Suplemento al Boletín Oficial* núm. 41, de 13 de Octubre de 1993(modificada por la Ley 2/2002. Publicada en el *Boletín Oficial*, núm. 21 de 27 de mayo de 2002 y por el art. 13 de la ley 7/97, de 2 de diciembre, publicada en el *Suplemento del Boletín Oficial* núm. 48 de diciembre de 1997).

datos personales para garantizar el honor, la intimidad personal y el pleno ejercicio de sus derechos.

5.5.1. La declaración de voluntad por medios electrónicos

Antes de acometer el análisis de las legislaciones guineanas sobre la declaración de voluntad, es esencial explicar en qué consiste dicha declaración. En este sentido, suscribiendo textualmente la tesis sostenida por algún autor, tras poner de relieve, que "la declaración de voluntad emitida electrónicamente no es sino un Mensaje de Datos, con variedad de configuraciones ---incluido el EDI— y métodos de firma electrónica (en adelante FE), que contiene la voluntad de comprometerse de su iniciador y signatario en el caso concreto"[699].

En la legislación guineana, el art. 217 del Código Civil (C.C) señala que la declaración de voluntad puede ser expresa o tácita, para ello se estará a lo siguiente: 1. será expreso, en su caso cuando la voluntad se manifiesta, por palabra, por escrito o por cualquier otro medio de manifestación directa. Y es tácita cuando se presume de los hechos.

En este sentido, es necesario que el legislador guineano redacte un nuevo precepto o que añada un nuevo párrafo del art. 217.1 del C.C, que admita el uso de los medios electrónicos como una forma de manifestación de voluntad. Por ser considerado como uno de los más importantes requisitos esenciales para la validez de los actos jurídicos manifestado a

[699] ILLESCAS ORTIZ, R. *Derecho de la…*op., cit., p. 215; también en «Oferta, perfección y prueba del contrato electrónico», en *Nuevas formas contractuales y el incremento del endeudamiento familiar*, núm. 50, Madrid: Consejo General de Poder Judicial, 2004, p. 226; según prevé el art. 2.2 del Modelo Europeo de acuerdo EDI (intercambio electrónico de datos), el Intercambio electrónico de datos se entenderá la transmisión electrónica de información de un ordenador a otra, de datos comerciales y administrativo que estructuran un mensaje de intercambio electrónico de datos con arreglo a una norma acordada, en *DOUE*, Nº L 338/100, de 28 de diciembre de 1994.

través de los medios electrónicos, a no ser que se puede presumir si no lo prohíbe. Es preciso añadir además que la manifestación de voluntad se puede expresar verbalmente, por escrito, medios electrónicos, o cualquier otra tecnología.

También, el art. 208 de la Ley uniforme sobre derecho general comercial (LUDGC) de la OHADA, prevé que el contrato de compraventa puede ser escrito o verbal; no está sujeto a ninguna exigencia de forma. En este sentido, dicho precepto no hace alusión a los medios electrónicos. Por lo que creemos imprescindible modificar el mencionado precepto 208 de la (LUDGC), que queda redactada de la siguiente manera:

En el contrato de compraventa la manifestación de voluntad se puede expresar verbalmente, por escrito, medios electrónicos, o cualquier otra tecnología.

Cabe resaltar que dichas propuestas no sólo contemplan el uso de los medios electrónicos como una forma de manifestación de voluntad, sino que deja abierta la posibilidad de que los avances tecnológicos no encuentren obstáculos para su incorporación al ordenamiento jurídico guineano.

Ha de concluirse que los efectos que producen la emisión de una declaración de voluntad a través de los medios electrónicos, son iguales cuando se trata de una declaración de voluntad emitida en forma escrita o verbal[700], "excepto aquellos contratos cuya perfección o validez de las leyes aplicables requieren la satisfacción de "escrituras formas o solemnidad".[701]

[700] Véanse, ILLESCAS ORTIZ, R. *Derecho de la…*op., cit., pp. 217 y ss; VEGA VEGA, J. A. *Contratos electrónicos y*…op., cit., p. 226 y ss. Para este autor, la "aparición y difusión de nuevas técnicas hace que los conceptos jurídicos tradicionales necesiten ser adaptados a las necesidades imperantes y, por consiguiente, la conversión del soporte puede servir para su percepción acústico o visual".

[701] ILLESCAS ORTIZ, R. *Derecho de la…*op., cit., p. 218.

5.5.2. Perfección de los contratos por medios electrónicos: Momento y Lugar

Cuando se trata de contratos celebrados presencialmente determinar el momento y lugar de perfección del mismo no plantea problema, dado que siendo la aceptación emitida y recogida casi simultánea, no hay intervalo durante el cual pueda dudarse si se ha verificado o no el encuentro de voluntades. Sin embargo, el tema se complica cuando los posibles contratantes se encuentran en lugares distintos y por tanto puede existir un intervalo de tiempo entre oferta y aceptación. El problema de determinar el momento de perfección del contrato es común de todos los contratos a distancia y no sólo de los contratos electrónicos, que además de electrónicos son contratos a distancia[702].

En los contratos electrónicos, como en los tradicionales, determinar el momento y el lugar en que se formaliza un contrato es importante con el motivo de establecer la capacidad de los contratantes, los plazos de acción y prescripción, la normativa jurídica aplicable, el correcto cumplimiento del contrato, la posibilidad de saber hasta qué momento pueden ser retiradas y revocada la oferta y aceptación[703].

Por último, es imprescindible que el legislador guineano tenga en cuenta en el momento de la modificación de las normativas jurídicas guineanas, así como en la elaboración de nuevas legislaciones, que los contratos celebrados electrónicamente, no representan nueva modalidad de contratos,

[702] Véanse, ARIAS POU, M. *Manual práctico de…*op., cit., p.201; vid. VEGA VEGA, J. A. *Contratos electrónicos y…*op., cit., p . 224; PARDO GATO, J. R. *Las cláusulas abusivas…*op., cit., pp. 440 y ss; FERNÁNDEZ PÉREZ N. *La contratación electrónica de servicios financieros*. Prólogo de Luis Fernández de la Gándara. Madrid: MARCIAL PONS, 2003, pp. 36 y ss.

[703] Véanse ARIAS POU, M. *Manual práctico de…,* op., cit., p. 202; DOMÍNGUEZ LUELMO, A., "contratación electrónica…"op., cit., p. 79;

sino que son los tradicionales celebrados por medios electrónicos, que es lo que determina su singularidad.

Nos centraremos ahora en analizar la normativa civil y mercantil de Guinea-Bissau, sobre el momento y lugar en la que un contrato se entiende perfeccionado.

A. *Momento de perfección del contrato electrónico*

Tanto en el Código civil como en la Ley uniforme sobre derecho general comercial, se contemplan y regulan diversos supuestos de perfección de los contratos[704]. Lo cierto es que la regla de perfección no es la misma para todos los supuestos. El momento de la conjunción de las declaraciones se puede producir en presencia de las partes contratantes o hallándose estos en lugares distintos, en este último caso, según la teoría de emisión o de la declaración, el contrato entre personas distantes se perfecciona en el momento en el que el aceptante declara su voluntad de aceptar la oferta de contratación propuesta[705].

[704] Para RODRÍGUEZ DE LAS HERAS BALLELL, "el momento de perfección del contrato es el que determinará el nacimiento de la relación contractual a la vida jurídica". RODRÍGUEZ DE LAS HERAS BALLELL. T «La formación del contrato en el entorno electrónico y los procedimientos electrónicos de contratación», en CALVO CARAVACA, Alfonso Luis; CARRASCOSA GONZÁLEZ, Javier, *Estudios sobre contratación internacional*, Madrid: Colex, 2006, pp. 535-572; Por su parte, el Profesor ILLESCAS ORTIZ, destaca que "la perfección contractual consiste en un acuerdo de voluntades sobre objeto de causa"; este mismo autor, señala que " hasta que no existe acuerdo no hay contrato", ILLESCAS ORTIZ R. *Derecho de la…*op., cit., p. 251; también en «Oferta, perfección y…op., cit., p. 234.

[705] Vid. DIEZ-PICAZO, L.; y GULLON, A. *Sistema de derecho civil. El contrato en general. La relación obligatoria*, vol. II, t. I. 12. ª ed. Madrid: Tecnos, 2012, pp. 62 y ss; ARIS POU, M. *Manual práctico…*op., cit., p. 203; según sostiene GONZÁLEZ GONZALO, se "entiende que el contrato se perfecciona cuando el destinatario de la oferta manifiesta o exterioriza la aceptación, pues en ese instante coexisten las declaraciones de voluntad que dan lugar al consentimiento requerido para la conclusión del contrato. Al mismo tiempo, aclara en la nota 373, que la declaración de la voluntad no exteriorizada es una mera intención de aceptar, un pensamiento carente de eficacia", GONZÁLEZ GONZALO, Alfonso*. La formación del contrato tras la ley de servicios de la sociedad de la información y de comercio electrónico*. Granada: Comares, 2004, pp. 118 y ss

La segunda teoría hace alusión a la teoría de expedición, tras sostener que el contrato puede perfeccionarse desde el momento en que el aceptante expide su aceptación al oferente. Para algún autor, dicha perfección no sucede "en el mismo momento de emitir la declaración de voluntad, sino en un momento posterior cuando el aceptante pone en camino del oferente su declaración de voluntad"[706].

Por su parte, la tercera teoría de la recepción, resalta que el nacimiento o la perfección del contrato se produce cuando la declaración del aceptante llega al domicilio o ámbito de interés del oferente, no basta por tanto, ni que la declaración se haya emitido ni que se haya conocido, es indispensable su llegada al domicilio o ámbito de interés del oferente[707]; o sea, no es necesario que el oferente sepa de su contenido, pues basta que llegue fehacientemente la aceptación al ámbito de acción o esfera del oferente.

Finalmente, la cuarta teoría es la de la cognición, conocimiento o información[708]. Según esta teoría, el contrato se perfecciona cuando el oferente tiene efectivo conocimiento de la declaración del aceptante. En este sentido, dicha teoría se basa en el principio de que toda declaración de voluntad es eficaz desde el momento que llega a su destinatario[709].

---

[706] ARIS POU, M. *Manual práctico…*op., cit., p. 204.

[707] Ibídem, p. 204; según se establece en el art. 18.2 de la Convención de las Naciones Unidas sobre los contratos de compraventa internacional de mercadorías (CNUCCIM), "la aceptación de la oferta surtirá efecto en el momento en que la aceptación de asentimiento llegue al oferente". Este precepto acoge la teoría de la recepción; igualmente el art. 23 CNUCCIM; al mismo tiempo el art. 3.3 del Modelo Europeo de Acuerdo de EDI, establece que "un contrato celebrado mediante el EDI se considerará celebrado en el lugar y momento en que el mensaje de EDI que contenga la aceptación de una oferta llegue al sistema informático del oferente"; o sea, este precepto acoge la teoría de recepción.

[708] Vid. DIEZ-PICAZO, L., y PONCE DE LEÓN, L., *Fundamentos de derecho…*op., cit., p. 320; DOMÍNGUEZ LUELMO, A. "contratación electrónica…"*op., cit.,* p. 79, según este autor, "seguir a la teoría de cognición puede conducir a resultados no deseados, por lo que parece más lógico entender que el contrato se perfecciona en el momento que la aceptación llega al buzón del oferente, sin necesidad que éste tenga un conocimiento expreso de la misma"; vid. PARDO GATO, J. R. *Las cláusulas abusivas…*op., cit., pp. 440 y ss.

[709] O sea, la teoría de conocimiento señala que para que la contratación se lleve a cabo, es necesario que la aceptación sea conocida por el destinatario, debe llegar a conocimiento

En efecto, el apartado 1 del art. 224 del C.C guineano, prevé que la declaración negocial dirigida a un destinatario es eficaz tan pronto que llega a su poder o a su conocimiento[710]. En este sentido, el legislador guineano acoge la teoría de recepción, pero se subordina a la teoría del conocimiento en relación a la conclusión del contrato. Por su parte, el apartado segundo de este mismo precepto prevé lo siguiente: que se consideran eficaces aquellas declaraciones de voluntad que no fueron recibidas por su destinatario por su propia culpa.

Por su parte, el art. 218 de la LUDGC, establece que una declaración de aceptación o cualquier otra manifestación de intención se considera recibida por el destinatario cuando se comunique verbalmente, o sea entregada por cualquier otro medio al destinatario en su empresa o en su domicilio social[711]. Efectivamente, la Ley uniforme sobre derecho general comercial de la OHADA acoge el criterio o la teoría del conocimiento, pero subordina ese conocimiento al momento de la recepción.

Según algún autor[712], cuando se trata de contratación electrónica las declaraciones de aceptación[713] o manifestación de intención no pueden considerarse conocidas o recibidas cuando llegan a la dirección del destinatario. La función que cumple la dirección del destinatario en los

---

de la persona a quien está dirigida, con lo cual se da la coincidencia de las declaraciones de voluntad, surgiendo en consecuencia, el consentimiento o voluntad común de ambos contratantes.

[710] En este sentido, el legislador guineano transcribe textualmente el art. 224.1 del Código Civil portugués.

[711] El art. 24 de la CNUCCIM, establece que "a los efectos de esta parte de la presente Convención, la oferta, la declaración, aceptación o cualquier otra manifestación de intención "llega" al poder del destinatario cuando se le comunica verbalmente o se entrega por cualquier otro medio al destinatario personalmente, o en su establecimiento o, si no tiene establecimiento ni dirección postal, en su residencia habitual".

[712] ZUMARÁN, Sandro. *Contratación electrónica.* [En línea] disponible en Internet: http://pttcontraelmundo.files.wordpress.com/2007/10/la-contratacion-electronica-corregido.pdf (última consulta, 26 de agosto de 2012).

[713] La aceptación es una declaración de voluntad emitida por el destinatario y dirigida al oferente mediante la cual aquél comunica a éste su conformidad con los términos de la oferta.

contrato tradicionales, es "específicamente la de probar la posibilidad en la que se encuentra el destinatario de conocer, desde el momento de su recepción, las declaraciones contractuales que le envíe el remitente a su dirección"

En palabra de algún autor[714], "el contrato se perfecciona en el momento en que el cliente recibe del proveedor, por medios electrónicos, un acuse de recibo de la aceptación del cliente y confirma la recepción de dicho acuse de recibo". Este mismo autor, señala que "el acuse de recibo se considera recibido y la confirmación se considera dada cuando las partes a las que se ha destinado estaban en disposición de acceder a los mismos".

Cabe decir, que no compartimos la tesis sostenida en el párrafo anterior, ya que es una postura errónea, porque hace depender la recepción de la voluntad y la acción de la otra parte. En este mismo sentido, para algunos autores, el acuse de recibo "no constituye nunca una declaración de voluntad. Su función en relación con el proceso contractual es meramente confirmativa. Por ello el acuse de recibo actúa siempre como una mera declaración de consentimiento: la confirmación de que ha llegado el mensaje del que se acusa recibo" [715].

B. Lugar de celebración del contrato electrónico

Es necesario regular en el Código Civil y en la Ley uniforme sobre derecho general comercial de la OHADA, el lugar de celebración del contrato cuando las partes se encuentran alejadas geográficamente. Porque dichas

[714] ESCOBAR ESPINAR, M. *El comercio electrónico…*op., cit., p. 306; en cambio, según se prevé en el art. 23 de CNUCCIM, que el contrato se perfeccionara en el momento de surtir efecto la aceptación conforme a lo dispuesto en la presente convención.

[715] RODRÍGUEZ DE LAS HERAS BALLELL. T*. El régimen jurídico*…op., cit., p. 277; también en, "Intermediación en la…"*op., cit*., p. 1258; «La formación del…» *op., cit*., pp. 535-572; así lo ha expresado el Profesor ILLESCAS ORTIZ, tras sostener que el acuse de recibo "consiste en un MD (mensaje de dato), contenedor de una declaración de ciencia en cuya virtud su iniciador, destinatario de un procedente MD, comunica al iniciador de este último la recepción del mismo", ILLESCAS ORTIZ R. *Derecho de la…*op., cit., pp. 233 y ss.

normativas no contemplan expresamente en sus respectivos preceptos el lugar de celebración del contracto[716]. En este sentido, debe quedar redactada de la siguiente manera:

--Si el oferente y aceptante no determina el lugar de celebración del contrato se entenderá celebrado en el propio lugar en que se perfeccione el acuerdo.

--En los contratos realizados por medios electrónicos deberán seguirse las siguientes reglas:

- Siempre que una de las partes intervinientes sea consumidor o usuario, se presumirá como lugar de celebración el domicilio o residencia habitual de éste.
- Si el oferente y el centro servidor es la misma persona, el lugar de celebración del contrato sería aquel donde se encuentra el prestador de servicios o el servidor.
- Cuando el oferente y el servidor no es la misma persona, el lugar estará determinado por el domicilio del primero.

En conclusión, creemos que los contratos celebrados mediante el uso de las nuevas tecnologías de información y la comunicación requieren por parte del legislador guineano la redacción de una normativa jurídica específica, que defina y califique los contratos celebrados por vía electrónica, regule los requisitos técnicos, jurídicos y reconozca su equivalencia funcional con los contratos tradicionales.

[716] El lugar de la celebración del contrato resulta imprescindible para determinar la competencia del tribunal que ha de conocer de los posibles pleitos y de la ley aplicable, en conflictos de Derecho interregional e internacional; vid. ILLESCAS ORTIZ R. *Derecho de la…*op., cit., pp. 266 y ss; PARDO GATO, J. R. *Las cláusulas abusivas…*op., cit., pp. 440 y ss; RODRÍGUEZ DE LAS HERAS BALLELL, T. «La formación del…» *op., cit*., pp. 535-572

5.6. Diagnóstico

La realización del diagnóstico se basó en el empleo de varias técnicas que incluyen consultas a expertos sobre la situación de los medios de pago en el país como, por ejemplo, a los funcionarios de las distintas entidades bancarias y financieras radicados en Guinea-Bissau, y la conformación de la matriz DAFO.

Los principales problemas a los que se enfrenta la implantación del comercio electrónico[717] y el uso de las tarjetas como medio de pago en Guinea-Bissau, radican sobre todo en: la no existencia en el ordenamiento jurídico guineano de disposiciones tendentes a regular con carácter general el comercio electrónico; la falta de infraestructura tecnológica para llevar a cabo dichas implantaciones[718]; el bajo nivel de bancarización del país; la falta de conocimiento del comercio electrónico; y la no existencia de un proveedor de servicio de la sociedad de la información y comercio electrónico, entre otros. Dicha situación de partida puede convertirse en un serio obstáculo para el desarrollo del comercio electrónico en Guinea-Bissau.

[717] Según el *Informe de la Reunión de Expertos sobre Estrategias en Materia de Comercio Electrónico para el Desarrollo*, celebrada en Ginebra, Suiza, entre el 10 y el 12 de julio de 2002, "entre las causas que separan a las naciones desarrolladas de los países en desarrollo en cuanto al empleo de este comercio y las TIC destacan: la falta de conocimiento del comercio electrónico y de esa tecnología y sus ventajas, falta de infraestructura de telecomunicaciones y de la conectividad a Internet, el hecho de no ser asequible el acceso a Internet, ausencia de marcos jurídicos y reguladores adecuados, falta de capacidad humana necesaria, no utilización del idioma nacional y el contenido local y la falta de conocimientos y de capacidad empresarial". [En línea] disponible en Internet: http://www.unctad.org/sp/docs/c2em11d3.sp.pdf (última consulta el 19 de 11 de noviembre de 2012).

[718] Vid. FERNÁNDEZ JURADO, Yolanda; y VAQUERO LAFUENTE, Mª Esther. *Las TIC y un desarrollo justo y responsable de los países en vías de desarrollo*. [En línea] Disponible Internet: http://www.eben-spain.org/docs/Papeles/X/sthr_Vaquro-buna.pdf (última consulta 12 de marzo de 2012).

5.7. Análisis estratégico para el desarrollo del comercio electrónico y el pago mediante tarjeta en Guinea-Bissau (Matriz DAFO)

Hemos de subrayar que para tener una visión general de la situación actual en Guinea-Bissau es imprescindible analizar cada una de los factores que la condicionan. La forma adecuada de hacerlo es mediante la matriz DAFO[719], herramienta utilizada para la formulación y evaluación de la estrategia. Generalmente es utilizada para empresas, pero igualmente puede aplicarse a personas o países. Es un instrumento de análisis cuantitativo que permite sintetizar informaciones relativas a las fortalezas y debilidades internas, en este caso de Guinea-Bissau, confrontando éstas con las oportunidades y amenazas que ofrece el entorno. También permite medir cuán fuerte o débil es el país, así como realizar el diagnóstico y formular las estrategias.

Finalmente, se ha de resaltar que la matriz DAFO es una herramienta que vincula la fase estratégica dentro del proceso de planificación[720].

5.7.1. Análisis Interno

Para llegar a diagnosticar internamente el país resulta imprescindible identificar las debilidades y fortalezas que definen su posición relativa, determinan su situación interna y dibujan el marco sociopolítico, económico-empresarial y normativo en el que se habría de desarrollar el proyecto de modernización.

---

[719] Vid. ÁLVAREZ SÁNCHEZ, J. M. "*La red como…"* op., cit., pp.117; LÓPEZ DE PRADO, Rosario. «Bibliotecas de museos en España: características especificas y análisis DAFO», en *Revista General de Información y Documentación (RGID)*, núm. 1, vol. 13, 2003, pp. 23 y ss; vid. ABASCAL ROJAS, Francisco**.** *El DAFO valora las debilidades, amenazas, fortalezas y oportunidades de la empresa.* [En línea] disponible en Internet. http://www.barcelonanetactiva.com/barcelonanetactiva/images/es/2_El%20analisis%20DAFOtcm106-22138.pdf (última consulta 5 de febrero de 2012).

[720] Vid. GROSS, Manuel. *Los orígenes del modelo de análisis DOFA* (actualizado). [En línea] disponible en Internet: http://manuelgross.bligoo.com/content/view/455327/Los-origenes-del-modelo-de-analisis-DOFA-actualizado.html (última consulta 22 de noviembre de 2012).

A. Debilidades

Identifica los recursos de los que se carece, las habilidades que no se poseen, las actividades que no se desarrollan positivamente. Es decir, aquellas características y capacidades internas del país que no están desarrolladas para contribuir al éxito sino que más bien provocan situaciones desfavorables[721].

Debilidades:

La insuficiente penetración de Internet en Guinea-Bissau. Según los datos recopilados por la Central de Inteligencia Americana (CIA), Guinea-Bissau ocupa el puesto 45 en África y el 173 a nivel mundial en número de usuarios de Internet, con 37.100 de usuarios en marzo de 2011[722].

Por otra parte, analizando los datos en términos relativos al índice de población, la cifra de usuarios de Internet en Guinea-Bissau representa únicamente el 2,3 % de la población[723], lo que sitúa el país por debajo de otros países miembros de la UEMOA, CEDEAO Y ODHA. Así, por ejemplo, Cabo-Verde cuenta con una cifra de penetración del 29,1% de la población,

[721] ORICH, Jessie M. *Análisis de FODA* [En línea] disponible en Internet http://manuelgross.bligoo.com/content/view/284581/Guia_para_el_analisis_FODA.htm (última consulta, 2 de noviembre de 2012); vid. ÁLVAREZ SANCHEZ, J. Ml. *La red…op., cit.,* p.117; Siguiendo las tesis sostenida por ABASCAL ROJAS, quien sostiene que "las debilidades quedan definidas como aquellos estrangulamientos o obstáculos que mientras no se eliminan, cuartan el desarrollo de otros presumibles puntos fuertes, al mismo tiempo que ayudan a resquebrajar el funcionamiento de la empresa por mayor debilitamiento de otras debilidades", en ABASCAL ROJAS, Francisco. *Como se hace un plan estratégico. Modelo de desarrollo de una empresa.* 2. ª ed. Pozuelo de Alcorcón (Madrid): ESIC Editorial, 1999, pp. 87 y ss.

[722] Estas informaciones fueron tomadas del sitio web del Central de Inteligencia Americana (CIA World Factbook). [En línea] disponible en internet: http://www.indexmundi.com/g/r.aspx?c=pu&v=118&l=es (última consulta 3 de noviembre de 2012); Unión Internacional de Telecomunicaciones, Informe sobre el Desarrollo Mundial de las Telecomunicaciones y base de datos; vid. http://www.economywatch.com/economic-statistics/Guinea Bissau/Internet_Users/(última consulta 3 de noviembre de 2012)

[723] *Estadísticas de Internet en África Marzo 31, 2011 (Población y Usuarios del Internet en África*)[En línea] disponible en Internet: http://www.exitoexportador.com/stats1.htm(última consulta el 18 de noviembre de 2012)

Senegal del 7,3%, Togo del 5.3 %, Nigeria del 28,3%, Ghana del 5,2%, Costa de Marfil del 4,5%, Camerún del 3,8%, Gabón del 6,3% y Comoros del 3,1%

Creemos que uno de los factores que explica que el país se ubique en este puesto es el alto costo de acceso a Internet, ya que una hora de conexión a Internet sobrepasa el ingreso medio diario de la población. Por lo tanto, para facilitar el acceso de la población a Internet es necesario reducir el precio de la conexión.

El aumento de la tasa de uso de Internet es un factor esencial para el desarrollo del comercio electrónico en el país. Por lo que es necesario ir aumentando paulatinamente el uso de Internet entre los jóvenes ya que en la medida en que este grupo poblacional vaya creciendo y transformándose en segmentos de población con mayor capacidad adquisitiva, el crecimiento del comercio electrónico pasará a ser exponencial[724].

Lentitud en el acceso a Internet. Esta variable se refiere el ancho de banda, que es la capacidad necesaria para el acceso a Internet. Es decir, está relacionada con la velocidad y eficiencia con que se accede y se trabaja en Internet.

Limitado números de servidores de acceso a Internet (infraestructura tecnológica). El número de servidores disponibles en Guinea-Bissau es de 82, según datos publicados en marzo de 2011[725].

[724] Sería una gran oportunidad para el país pertenecer el grupo de los países en la que pasará el cable de telecomunicaciones submarino en 2012 el que hará escala en la isla española de Tenerife y que conectará toda la costa occidental de África atravesando 20 países, escuelas y hospitales de ese continente dispondrán de banda ancha y podrán conectarse al mundo[724]. Sin embargo, Guinea-Bissau no está incluido dentro de ese grupo.

[725] esta información fue actualizado en marzo de de 2012 http://www.indexmundi.com/map/?t=0&v=140&r=af&l=es(última consulta, 8 de noviembre de 2012).

Falta de una legislación para impulsar el comercio electrónico. La no existencia de un marco jurídico legal (por ejemplo: legislación sobre firma electrónica, servicios de pago, protección de consumidores y usuarios y, en general, servicios de la sociedad de la información y comercio electrónico), que garantice la seguridad en la transacción electrónica y en la operación de pago mediante tarjeta de crédito o débito, representa un freno para el desarrollo del comercio electrónico en el país.

El bajo nivel de bancarización. Puede ser un freno para la implantación del comercio electrónico en la medida en que paralizaría el uso de los medios de pago electrónicos para completar las transacciones en la fase de ejecución. Cabe señalar que actualmente existen cuatros entidades bancarias comerciales operando en el país: Banco de África Occidental (BAO), Banco Regional de Solidaridad (BRS), Banco de la Unión (BDU) y Banco Panafricano (Ecobank).

Recursos humanos no cualificados. Se constata una apreciable escasez de capital humano altamente cualificado que pueda responder a las necesidades y atender las exigencias de una implantación progresiva del comercio electrónico en el país.

La inestabilidad política y económica. Se hace referencia a esta variable de riesgo para el país en la medida en que puede ejercer una influencia negativa para el desarrollo del comercio al poner en riesgo la seguridad del tráfico y, en particular, la implementación del comercio electrónico en el país.

La falta de conocimiento por parte de la población de los riesgos y las condiciones para efectuar pagos a distancia. Por lo que el fraude aumentaría, sobre todo, en las siguientes modalidades: phishing, código malicioso, pharming y cartas nigerianas.

B. Fortalezas

Son las capacidades especiales con las que cuenta el país que le confieren una posición privilegiada para abordar el proyecto de modernización e implantación planteado en este trabajo. Comprenden los recursos que se controlan, las capacidades y habilidades que se poseen y las actividades que se desarrollan positivamente. Señalaremos:

La pertenencia a organizaciones regionales. En este sentido, puesto que el país es miembro de la UEMOA, CEDEAO, OHADA, se puede beneficiar de las tareas de armonización de las distintas legislaciones que hemos referido a lo largo de este epígrafe[726].

Un país en crecimiento. Al no contar con legislación en la materia está abierto a la elaboración de una legislación muy depurada técnicamente, que contraste modelos ya existentes y puestos a prueba y que, al ser un territorio en el que las cifras de comercio electrónico van a dispararse necesariamente en un futuro muy próximo.

Su extensión territorial. El ser uno de los países más pequeños de África continental le permite gestionar mejor las soluciones. Además, la no existencia de diferentes legislaciones en el país facilita la implementación de leyes en todo el territorio nacional; es decir, por el tamaño y la división administrativa del país no existe el derecho interterritorial o interregional, como existe en otros.

5.7.2. Análisis Externo

Para realizar este análisis se deben identificar las oportunidades y amenazas del entorno.

[726] Vid. ABASCAL ROJAS, Fco. *Como se…*op., ciit., p. 88

A. Oportunidades

Son aquellos factores o variables que resultan positivos, favorables, explotables para el país y que permiten obtener ventajas competitivas[727] para afrontar el reto de la electrónificación.

Comodidad que brindaría el comercio electrónico entre empresa y usuario (B2C) en el país. Permitirá al consumidor o usuario de la tarjeta acceder desde cualquier lugar a un amplio rango de productos y servicios, simplemente disponiendo de una conexión a Internet[728].

El alto nivel de la seguridad en la tarjeta de crédito o débito que incorpora chip. Este tipo de tarjeta es la perteneciente al sistema EMV (Europay Mastercard Visa) e introduce un estándar de calidad con circuito integrado, que se basa en la criptografía. Son las llamadas tarjetas inteligentes que están reemplazando a las tarjetas de banda magnética. El chip sí permite aportar tratamiento criptográfico al proceso porque es un dispositivo que genera criptogramas[729]. Por tanto, el país podría optar por incorporar la tecnología más sofisticada y fiable y de ese modo mejorar la seguridad de todo el sistema.

El uso del sistema SET o el 3D Secure. La utilización de estos protocolos o mecanismos garantizarían la seguridad en las operativas de pago mediante tarjeta en el comercio electrónico seguro en Guinea-Bissau.

El surgimiento de nuevas empresas en el comercio electrónico o la incorporación de las empresas tradicionales ya existentes en el país. La creación de las nuevas empresas en el comercio electrónico permite ahorros de costos en infraestructura física para la venta. Por otro lado, el

[727] http://es.wikipedia.org/wiki/An%C3%A1lisis_DAFO(última consulta 13 de noviembre de 2012).
[728] ALONSO CONDE, A. B. *Comercio electrónico*…op., cit., p. 21.
[729] ADICAE. *Catálogo técnico*…op., cit., p. 20.

comercio electrónico tiene la capacidad de potenciar una mejor inserción de la empresa en el mercado, ampliando su demanda potencial y permitiéndole acceder a t ecnologías que sólo estaban disponibles para las grandes empresas debido a su alto costo.

Acceso al mercado global. La implementación de un comercio electrónico B2C permitirá a los futuros consumidores y usuarios guineanos acceder a cientos de tiendas virtuales existentes en todo el mundo, con el objetivo de facilitarles la adquisición de bienes o servicios que no están disponibles en el territorio guineano.

B. Amenazas

Son aquellas situaciones que provienen del entorno externo y que pueden transformarse en amenazas para el comercio electrónico en Guinea Bissau.

La falta de presencia física simultánea de las partes contratantes. Impide la identificación de los sujetos intervinientes en una transacción, situación que puede traer consigo el uso fraudulento o indebido de la tarjeta en la futura operativa de pago realizada desde el ordenador del cliente ubicado en Guinea-Bissau.

Elevado nivel de riesgo en la operativa de pago mediante tarjeta en Internet en Guinea-Bissau. Esta variable se refiere a la vulnerabilidad de la comunicación de los datos de la tarjeta a través de Internet en la medida en que pueda ser interceptada por terceros que podrían utilizar aquellos para cometer actos fraudulentos o indebidos, incluso sin ser identificados.

El *ataque a los sitios web mediante la inyección SQL y XSS*. En este caso, el atacante puede introducir un script en una base de datos SQL mediante un formulario basado en web o inyectar malware en páginas

web[730] y de este modo suplantar el comprador y el proveedor de bienes o servicios (servidor de pago).

Esta variable traería consigo la falta de confianza de los consumidores y usuarios, así como de los prestadores de bienes o servicios en Internet.

Tabla: 1 de la Matriz DAFO

Fuente: elaboración propia

[730] CASTRO BROTTO, Leonardo. *Los sitios de comercio electrónico enfrentan nuevas amenazas*. [En línea] Disponible en Internet: http://la.trendmicro.com/la/about/news/pr/article/20081117164206.html(última consulta 25 de octubre de 2012). El atacante puede dañar datos contenidos en los sitios web (como números de tarjetas de crédito) o robar la identidad de quienes se hayan registrado en él, además de modificar el contenido del sitio. Al aprovechar las vulnerabilidades existentes en los sitios web legítimos, los atacantes pueden lograr que empresas afectadas se convierta sin saberlo en cómplices de diseminar spyware o participar en el robo de identidades. Esto puede poner en peligro los ingresos de su negocio, los datos de sus clientes y su reputación como compañía.

5.8. Procedimiento de la matriz DAFO

Una vez seleccionadas las variables se calcula el coeficiente de correlación entre ellas para conformar la matriz DAFO. Ésta se determina según los impactos o combinaciones y según la relación entre las variables por cuadrantes a partir de la siguiente escala:

3 significa influencia fuerte,

1 influencia débil

2 influencia media

-3 influencias fuertes negativas; y

Cuando es 0 significa nula.

Las combinaciones se basan en las siguientes preguntas:

CUADRANTE I ¿Qué hacer para disminuir o eliminar nuestras debilidades y aprovechar las oportunidades que se nos presentan?

CUADRANTE II ¿Qué hacer para disminuir o eliminar nuestras debilidades y atenuar las amenazas que nos rodean?

CUADRANTE III ¿Qué hacer para utilizar nuestras actuales fortalezas a fin de aprovechar las oportunidades?

CUADRANTE IV ¿Qué hacer para utilizar nuestras fortalezas a fin de enfrentar o atenuar las amenazas?

Tabla2. Matriz DAFO

DEBILIDADES	OPORTUNIDADES(DO) I							AMENAZAS(DA) II					
		1	2	3	4	5		1	2	3	4	5	
	1	-3	0	0	-3	-3		0	0	0			
	2	-3	0	-2	-3	-3		0	0	0			
	3	-3	0	0	-3	-3		0	0	0			
	4	-3	-3	-3	-3	-3		-3	-3	-3			
	5	-3	0	0	-3	-3		0	0	0			
	6	-3	-3	-3	-3	-3		-2	-2	-2			
	7	-3	0	0	-3	-3		0	0	0			
	8	-3	-3	-3	0	0		-3	-3	-3			
	OPORTUNIDADES(FO) III							AMENAZAS(FA) IV					
FORTALEZAS		1	2	3	4	5		1	2	3	4	5	
	1	3	3	3	3	3		0	0	0			
	2	3	0	0	3	3		0	0	0			
	3	2	0	0	0	0		0	0	0			

Fuente: elaboración propia.

Una vez definidos los impactos y su magnitud se procede a la proyección de las estrategias teniendo en c onsideración su ubicación, según el cuadrante:

CUADRANTE I. Estrategia adaptativa(*DO*).

CUADRANTE II. Estrategia de supervivencia(*DA*).

CUADRANTE III. Estrategia de carácter ofensiva (*FO*).

CUADRANTE IV. Estrategia de carácter defensiva (*FA*).

5.9. La estrategia

Como se puede observar, el mayor porcentaje de los impactos negativos se ubican en el cuadrante I. Por lo tanto, el gobierno debe adoptar una estrategia adaptativa porque el país cuenta con un conjunto de debilidades que debe eliminar con objeto de aprovechar las oportunidades que el entorno le brinda, logrando atenuar las amenazas y superar sus debilidades.

Esta estrategia fue seleccionada después de haber realizado el análisis de los impactos de la matriz DAFO y está en correspondencia plena con el objetivo general de este capítulo que es determinar la conveniencia o no de la implementación del comercio electrónico en Guinea-Bissau, por lo que el país debe eliminar rápidamente sus debilidades, utilizando las fortalezas que posee para aprovechar las oportunidades que brinda el entorno, y minimizando las amenazas.

Esto anima a todos los actores en lo que al uso de comercio electrónico se refiere (al gobierno, entidades emisoras de los medios de pago electrónico, operadores de Internet, tribunales, proveedores de acceso a Internet que operan en el país) a trabajar fuertemente en la minimización de todas sus debilidades para aprovechar las oportunidades, basándose sobre todo en programas de acciones específicas y a reorientar sus estrategias.

Las estrategias orientadas a la reducción de las debilidades aprovechando las oportunidades y minimizando las amenazas (DO-A) pudieran ser del siguiente orden:

Se debe garantizar la penetración de Internet mediante la reducción del costo de acceso con el fin aprovechar la comodidad que brinda el comercio

electrónico y eliminar la falta de conocimiento de la población para realizar compras por Internet.

El gobierno debe redactar un marco jurídico legal que discipline todas aquellas actividades relacionadas con el comercio electrónico seguro, especialmente el pago mediante tarjeta de crédito en el comercio electrónico, así como el pago a través del dispositivo móvil, para que los sujetos intervinientes en la operativa de pago puedan aprovechar las comodidades que ofrece el comercio electrónico seguro y así utilizar el alto nivel de seguridad en las tarjetas que incorporan chip para atenuar los riesgos relacionados con la falta de presencia física simultanea de las partes, así como el elevado nivel de riesgo en la operativa de pago electrónico en Internet.

Trazar planes de capacitación que den respuesta a las necesidades de los recursos humanos, prioritariamente de los sectores y actividades vinculadas al comercio electrónico y el pago mediante tarjeta en Internet para poder aprovechar las oportunidades del comercio electrónico y el pago electrónico, y fomentar el surgimiento y la consolidación de nuevas empresas dedicadas al comercio electrónico o que ofrecen sus productos o servicios a través de la red, así como el acceso al mercado global, con el fin de atenuar la falta de confianza de los consumidores y prestadores bienes o servicios en el comercio electrónico.

Garantizar la estabilidad política y económica para poder aprovechar la comodidad que brinda el comercio electrónico a nivel global y disminuir la falta de confianza que puede generar esta inestabilidad.

Se debe admitir que el país se encuentra en una etapa de inestabilidad política y económica, motivada por una serie de factores internos y externos vistos anteriormente. Debido a la importancia o al beneficio que el comercio

electrónico puede reportar al país, se hace necesario, ante todo, crear una nueva cultura o forma de pensar y realizar estrategias basadas fundamentalmente en el proceso de gestión por valores y con la filosofía de que todos los implicados ganen. Con este resultado de suma positiva, no ganará solamente el país sino también todos aquellos que de una forma u otra participen en los beneficios de éste, y donde la capacidad y el talento del más alto liderazgo dentro del país se constituya en la clave del éxito.

El comercio electrónico seguro debe convertirse en la perspectiva y espíritu de esfuerzo del país y además debe ser aceptado por los guineanos como una de las vías para reducir la pobreza y facilitar las relaciones comerciales. Por otra parte, es necesario destacar la importancia que reviste para el país la redacción y aprobación de disposiciones jurídicas que regulen el comercio electrónico y todos los servicios que coadyuvan a su desarrollo, en especial los servicios de pago, de entre los cuales nos interesa en particular, por su demostrada multifuncionalidad, el pago con tarjeta.

Más adelante se desarrolla como parte de la estrategia un grupo de normativas que regulan el uso de la tarjeta como medio de pago en el comercio electrónico con el fin de garantizar la seguridad en las operativas de pago mediante tarjeta en Internet que podrían tomarse como referencia para su implantación en Guinea-Bissau.

Es necesario, al iniciar esta tarea, no olvidar que las opciones que se manejen no pueden ser ajenas a la misión, a la visión y a los objetivos definidos.

La misión: es la finalidad fundamental que justifica la existencia de un país y es el punto de partida en la formulación de la estrategia. O sea, la misión es la razón de ser de la organización, la meta que moviliza las energías y capacidades, es la base para procurar una unidad de propósitos en los actores con el fin de desarrollar un sentido de pertenencia y expresa

el aporte más importante y significativo de la sociedad. A continuación se le da a conocer la misión al gobierno y las entidades bancarias:

Contribuir al desarrollo económico y social de Guinea-Bissau a través de la implementación de un modelo de comercio electrónico seguro tal como funciona en España.

La visión: significa trabajar con el objetivo de hacer cumplir las expectativas del país a partir de los requerimientos de las estrategias diseñadas, estimulando el comercio electrónico y el pago mediante tarjeta en Internet, en busca de un incremento acelerado de la economía y la sociedad para reducir el nivel de pobreza actual.

Áreas de resultados clave para el comercio electrónico en Guinea-Bissau: contratación electrónica, ventas y compras de productos, transacciones electrónicas y seguridad jurídica y técnica

5.10. Determinación de escenarios

En este caso se ha considerado la valoración de un sólo escenario[731] alternativo: se implementa el comercio electrónico y el pago mediante tarjeta en Internet en el medio plazo (hasta el 2018). Este escenario implica que hasta el 2018 se apueste por incrementar las posibilidades de acceso a Internet a corto y medio plazo, y aumentar la afluencia de las entidades bancarias, proveedores de acceso a la red, proveedores de servicios de certificación y proveedores de bienes o servicios.

[731] El método de escenarios es una herramienta que se emplea en análisis de problemas o situaciones cualitativas. El mismo permite incluir en las investigaciones factores que los métodos tradicionales no podían tener en cuenta, como por ejemplo: la situación política y económica del país; la pobreza y la corrupción, etc…

5.11. Plan de acción.

El plan de acción es el conjunto de tareas que es necesario ejecutar dentro de la estrategia para dar cumplimiento a los objetivos estratégicos proyectados. Se basa en la elaboración de acciones específicas para las áreas de resultados clave del país, a fin de alcanzar los objetivos previstos en las estrategias diseñadas. Para desarrollar estos planes, se debe planificar, organizar, liderar y controlar todas sus acciones. En otras palabras, se puede decir que en este caso es muy importante definir qué hay que hacer.

Antes de responder dicho interrogante, es necesario, en primer lugar, hacer algunas aclaraciones sobre lo que hemos venido resaltando con anterioridad, es decir, la no existencia de normas jurídicas sobre comercio electrónico en Guinea-Bissau.

No obstante, cabe destacar que el país cuenta con regulaciones que se pueden aplicar en los pagos tradicionales, por ejemplo el Código civil que recoge como régimen general las obligaciones[732] y la responsabilidad[733] de las partes interviniente en una relación jurídica.

Y por otro lado, el Acto uniforme relativo al derecho comercial general firmado por los países miembros de la OHADA, que establece en su Título III, Capítulo II, Sección I, la obligación del comprador sobre pago de precio (art.233 y ss.)

Igualmente, el Reglamento Nº 15/2002/CM/UEMOA de sistema de pago en los Estados miembros de la Unión Económica Monetaria del África Occidental, que hemos señalado con anterioridad, aborda cuestiones relacionadas con certificado electrónico, firma electrónica, cheque, letra de

[732] Vid, art. 397 del Código civil de de la República Guinea-Bissau
[733] Ibídem, art.483 del Código civil

cambio y tarjeta de pago. Además, en su Sección I se establecen las obligaciones y responsabilidades de las partes en la transferencia electrónica de fondos (artículos 133, 134,135 y 136[734]). Este mismo Reglamento Nº 15/2002/CM/UEMOA prevé en su Capítulo II, Sección I, todo lo relacionado con la prevención del fraude, el abuso y la falsificación de tarjeta bancaria, instrumentos y métodos de pago electrónico. Sin embargo, esta normativa aún no ha sido adaptada al derecho interno guineano.

Desde nuestro punto de vista, sería viable y oportuno que el legislador guineano elabore tres marcos normativos y regulatorios que agrupen todas aquellas actividades relacionadas con el comercio electrónico y, en particular el pago mediante tarjeta de crédito. Por ejemplo:

1. *Ley de Servicio de la Sociedad de la Información y Comercio Electrónico*

En el país no existe ninguna normativa jurídica que regule los servicios de la sociedad de la información y el comercio electrónico. Sin embargo, para la implementación del comercio electrónico y el pago mediante tarjeta de crédito en Internet en Guinea-Bissau, resulta obligatoria su regulación.

Por ello, el legislador guineano deberá ser lo más exhaustivo posible respecto a los actos o actividades que pueden ser considerados servicios de la sociedad de la información[735] y los que no[736], así como aquellos actos que

[734] Según se prevé en el art. 136 del Reglamento Nº 15/2002/CM/UEMOA, las relaciones entre el emisor y el titular de la tarjeta u otro instrumento pago electrónico y el beneficiario se rigen por el acuerdo de las partes.

[735] En este sentido, el legislador guineano debe tener en cuenta que para calificar un servicio como servicio de la sociedad de la información deben concurrir tres requisitos: Titulo oneroso/Actividad económica, prestación a distancia y por vía electrónica; y a petición del destinatario.

-*Titulo oneroso/Actividad económica*: es la primera de las características que debe concurrir en un servicio para ser considerado dentro de la categoría de servicio de la sociedad de la información. Se considera que una actividad es prestada a título oneroso cuando se realiza a cambio de una remuneración económica y se suministra de tal manera que la actividad suponga recíprocas prestaciones entre el adquiriente y el transmitente.

pueden ser contrarios al Derecho, describiendo un supuesto general, que sea capaz de incluir toda conducta de esta índole, evitando así las consecuencias de la laguna legislativa de determinados supuestos.

Seguidamente, deberán regular las diversas causas que se puede reconducir al régimen general de responsabilidad de los proveedores de contenido y prestadores de servicios de intermediación. La incorporación legislativa de un cuerpo normativo de esta naturaleza en nuestro país es indispensable dada la importancia que juega el comercio electrónico en la economía a nivel mundial.

2. *Ley de servicios de pago electrónico*

También será imprescindible desarrollar una ley de servicios de pago electrónico que deberá incorporar un sistema común de derechos, obligaciones y reglas de responsabilidades para proveedores y usuarios en relación con la prestación y utilización de los servicios de pago.

Por otra parte, creemos que sería viable que el legislador incluyera dentro de esta ley preceptos relacionados con la protección de los consumidores titulares de medios de pago electrónico. Ya que es

---

-*A distancia*: un servicio suele ser prestado a distancia cuando se lleva a cabo y produce sus efectos sin que las partes estén presentes simultáneamente.

-*Por vía electrónica:* estamos ante un servicio prestado por vía electrónica cuando es enviado en el origen y recibido en el destino a través de los medios electrónicos de procesamiento y de almacenamiento de datos, que sean íntegramente trasmitido y recibido por cable;

- *A petición individual del destinatario de los servicios*: es decir punto a punto y no los que se prestan punto-múltiple.

[736] Según se establece en la LSSSICE, no son considerados servicios de la sociedad de la información, aquellos servicios prestados por medios de telefonía vocal, fax o telex; el intercambio de información por vía de correo electrónico u otro medio de comunicación electrónica similar para fines ajenos a la actividad económica de las personas que lo utilizan; los servicios de radiodifusión televisiva (incluidos los servicios de cuasi-video a la carta). También no son considerados servicios de la sociedad de la información, aquellos servicios prestados por los notarios, registradores de la propiedad mercantiles, los abogados y procuradores en el ejercicio de sus respectivas funciones públicas (art. 5 a) y b) LSSICE).

.

fundamental garantizar la protección de los consumidores y usuarios titulares de medios de pago electrónico en cuanto al uso fraudulento o indebido de la tarjeta de crédito o débito en el comercio electrónico.

Además, es necesario regular de forma detallada las cláusulas abusivas para detectarlas e imponer su no inclusión, regulando la responsabilidad de los sujetos intervinientes en el contrato de adhesión ante un posible fraude, no dejándolo como venían sucediendo en el derecho español a la voluntad de las partes, como se pudo comprobar a lo largo de esta investigación. En tal sentido, resulta significativa la incorporación de las reglas sobre la carga de prueba explicada en el capítulo III y IV de esta investigación.

También se recomienda que el legislador introduzca en la redacción de esta normativa lo referente al pago por móvil.

3. La ley de firma electrónica

Es necesario hacer énfasis en algunos otros aspectos novedosos que deberían ser estructurados en nuestro ordenamiento jurídico. Por ejemplo, la necesidad de crear una normativa jurídica sobre firma electrónica para reforzar la confianza de los consumidores y usuarios titulares de la tarjeta, ya que la firma electrónica resulta ser un instrumento imprescindible para la comprobación de la procedencia e integridad de los datos intercambiados entre las partes intervinientes en la operativa de pago en Internet y para la celebración de transacciones electrónicas.

Asimismo, resulta especialmente destacable señalar que la utilización de la firma electrónica reconocida puede contribuir a atenuar las amenazas o riesgos en la operativa de pago en el comercio electrónico, especialmente en Internet. En esta misma línea, se ha de resaltar la importancia de realizar investigaciones sobre la procedencia y valor de la firma electrónica y la actuación de los prestadores de servicios de certificación en las

transacciones electrónicas o en la operativa de pago mediante tarjeta en el comercio electrónico a fin de brindar a las partes intervinientes mayor seguridad.

Además, es necesario para el desarrollo del comercio electrónico que el legislador guineano tenga en cuenta a la hora de redactar la ley, la inclusión de los principios o reglas generales aplicables a todo tipo de comercio electrónico. Los principios a lo que nos estamos refiriendo son[737]:

- Principio de equivalencia funcional
- Principio de neutralidad tecnológica[738]
- Principio de inalteración del derecho preexistente de obligaciones y contratos[739]

[737] ILLESCAS ORTIZ, R. "Los principios de la contratación electrónica, revisitados", en MADRID PARRA, A; GUERRERO LEBRÓN, María Jesús (Coords.). *Derecho patrimonial y tecnología: revisión de la contratación electrónica con motivo del Convenio de las Naciones Unidas sobre Contratación electrónica de 23 de noviembre de 2005 y de las últimas novedades legislativas.* Madrid: Marcial Pons, 2007, pp. 21-38; también, *Derecho de la*…op., cit., pp. 37-58; vid., la SJPI núm.2, de Castellón de 25 de junio de 2008(*AC*/2008/1621); vid. MATEU DE ROS, R. "Principios de la contratación electrónica en la Ley de servicios de la sociedad de la información y el comercio electrónico", en MATEU DE ROS, R.; y GALLEGO, Mónica López-Monís (coords.). *Derecho de Intente. La Ley de servicios de la sociedad de la información y de comercio electrónico.* Prólogo de Carlos López Blanco. Cizur Menor (Navarra): Aranzadi, S.A., 2003, pp. 71-104; GONZÁLEZ-MENESES, Manuel. *La firma electrónica como instrumento de imputación jurídica. Una reflexión de Derecho civil sobre la contratación electrónica*, Madrid: Colegio Notarial de Madrid, 2010, p. 12 y ss.

[738] Según pone de relieve el Profesor ILLESCAS ORTIZ, la neutralidad tecnológica es "aquella aptitud que debe imperar en las nuevas normas disciplinadoras del C-E para abarcar con sus reglas no sólo las tecnologías existentes en el momento en que se formulan sino también las tecnologías futuras sin necesidad de verse sometidas a modificación. Ello, obviamente, en un horizonte cronológico razonable: desde luego dicho horizonte no es el horizonte más que bicentenario del código Napoleón pero tampoco podía ser el de una decena de años y ha si ha podido ser comprobado ante la permanente utilidad de las soluciones jurídicas incorporadas a la LMUCE y su perduración transcurriendo sobradamente el primer decenio de su existencia. A su vez, este autor sostiene que las tecnologías electrónicas incipientes están comprendidas por las normas en las mismas medidas y extensión en que lo están las tecnologías plenamente operativas (…). Las normas reguladoras del C-E y sus contratos han de resultar aplicables al C-E y no a una concreta tecnología de entre las disponibles en el mercado para la práctica de los intercambios comerciales a través de soporte electrónico", ILLESCAS ORTIZ, R. *Derecho de la*…op., cit., pp. 54 y ss.

- Principio de buena fe
- Principio de libertad de pacto.

La elaboración de estas normativas mencionadas con anterioridad se debe basar sobre todo en el modelo español, pero subsanando errores en algunos preceptos. Por ejemplo, el párrafo primero del art. 106 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU), establece para los "pagos mediante tarjeta", que "cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente, utilizando el número de una tarjeta de pago, el consumidor o usuario titular de la podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del empresario y del consumidor y usuario titular de la tarjeta se efectuarán a la mayor brevedad".

Teniendo en cuenta lo planteado por el legislador español en el precepto comentado en el párrafo anterior, a nuestro juicio, el legislador se quedó corto dado que no llega a establecer de forma explícita el plazo concreto para la devolución del importe cargado fraudulenta o indebidamente. O sea, se limita a indicar que el consumidor o usuario titular de la tarjeta podrá exigir la inmediata anulación del cargo y que las correspondientes anotaciones de adeudo y reabono (…) se efectúan a la mayor brevedad.

En este sentido, se ha de sostener que no existe ningún precepto, ni en la LRLOCM, ni en el TRLGDCU que regule el plazo para que el consumidor o usuario titular de la tarjeta ejerza el derecho a reclamar la anulación del importe cargado de modo fraudulento o indebido. Ante este vacío legal

[739] RODRÍGUEZ DE LAS HERAS BALLELL, T. «*Intermediación en la…o., cit.* pp. 217-259.

habría que recurrir, por analogía, al precepto 104 del TRLGDCU[740] en el que se establece un plazo que no deberá superar los 30 días para la devolución al consumidor y usuario de las cantidades abonadas.

Desde nuestro punto de vista, es conveniente proponer la modificación del apartado primero de este mismo art. 106 del TRLGDCU o que se añada un segundo párrafo en el cual se establezca un plazo de quince días naturales, ampliables a treinta días, para la devolución del importe cargado de modo fraudulento o indebido, evitando así la utilización de criterios por analogía que ni siquiera abordan cuestiones relacionadas con lo señalado en el párrafo primero de este mismo art.106 del TRLGDCU.

De este modo, se ha de resaltar que para la implementación del modelo español en Guinea-Bissau, es imprescindible establecer de forma explícita el plazo de la devolución del importe cargado de modo fraudulento o indebido en una futura ley de protección de los consumidores y usuarios de tarjeta de pago.

En segundo lugar, para la ejecución de este modelo es importante realizar labores de capacitación a los funcionarios de diversas instituciones del Estado, como por ejemplo a jueces, fiscales y policías judiciales, para que tengan conocimientos básicos sobre el servicio de la sociedad de la información y el comercio electrónico.

En tercer lugar, introducir el comercio electrónico y el Derecho de la contratación como una asignatura en las carreras de Economía y Derecho.

[740] Según se prevé en el art. 104 TRLGDC, "en caso de no ejecución del contrato por parte del empresario por no encontrarse disponible el bien o servicio contratado, el consumidor y usuario deberá ser informado de esta falta de disponibilidad y deberá poder recuperar cuanto antes, y en cualquier caso en un plazo de 30 días como máximo, las sumas que haya abonado"; Véanse BERCOVITZ RODRÍGO-CANO, R.: "Ventas a…"*op., cit.*, p. 729; FERNÁNDEZ PÉREZ, N.: "*El nuevo régimen…"op., cit.,* pp. 344-335.

En cuarto lugar, creemos que es necesario crear una entidad pública on line que se encargue de impulsar el desarrollo de la sociedad de la información y el comercio electrónico y ejecutar proyectos de acuerdo a las necesidades del país.

Y por último, cabe destacar la necesidad de realizar intercambios de experiencias con las universidades españolas, especialmente con la Universidad Carlos III de Madrid en el sector del comercio electrónico ya que dicha Universidad cuenta con profesionales altamente capacitados en la materia a través de los cuales podemos aprender mucho sobre el servicio de la sociedad de la información y el comercio electrónico.

5.12. El pago mediante tarjeta en el comercio electrónico en Guinea-Bissau

A nuestro juicio, no se puede hablar del pago mediante tarjeta en el comercio electrónico en Guinea-Bissau ya que el país carece de la infraestructura así como del marco legislativo que regule dicho pago. La infraestructura de pago en el comercio electrónico en Internet no está desarrollada. También cabe señalar que las instituciones bancarias y financieras no están informatizadas para permitir la banca electrónica y el pago por Internet.

De los pocos bancos que operan en el país, solo uno de ellos emite tarjetas de crédito[741], y hay otro que solo emite tarjetas de débito como medio de pago y puede ser utilizado fuera del país[742]. Lo cierto es que en la sociedad guineana la gente está más acostumbrada a la utilización del dinero efectivo para la mayor parte de sus transacciones debido a la inexistencia de una cultura bancaria.

[741] BRS es la entidad bancaria que emite tarjeta de crédito para el uso nacional y en la zona de la UEMOA.
[742] BAO esta entidad emite tarjeta de débito visa.

Por otro lado, la insuficiencia del entorno financiero se convierte así en uno de los obstáculos principales para el desarrollo de un sistema de pago electrónico seguro en Guinea-Bissau. En esta misma línea, se ha de hacer hincapié en que todo esto se atribuye a la falta de una política bancaria y a la debilidad de las organizaciones comerciales y financieras que operan a nivel nacional. Además, la falta de capital financiero dificulta la creación de una empresa para el comercio electrónico seguro.

El Estado guineano ha hecho poco para establecer una política eficiente de creación de entidades bancarias y así promover o atraer bancos extranjeros para invertir en el país. No existe ningún proyecto o iniciativa relacionada con la implantación del comercio electrónico seguro basado en el pago mediante tarjeta de crédito o débito. Por lo que se ha de insistir en la necesidad de implantar dicho modelo, basado en el ordenamiento jurídico español, que cuenta en la actualidad con un conjunto de importantes disposiciones tendentes a regular con carácter general el pago mediante tarjeta en el comercio electrónico seguro.

Una de estas disposiciones es la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, en la que "se introducen una serie de modificaciones tanto de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, como de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que constituyen dos piezas angulares del marco jurídico en el que se desenvuelve el desarrollo de la sociedad de la información". Mediante dicha normativa se aprueban una "serie de iniciativas normativas dirigidas a eliminar las barreras existentes a la expansión y uso de las tecnologías de la información y de las comunicaciones y para garantizar los derechos de los ciudadanos en la nueva sociedad de la información".

Al mismo tiempo debe destacarse la más reciente Ley 16/2009 de servicios de pag o, que establece un sistema común de derechos y obligaciones para proveedores y usuarios en relación con la prestación y utilización de los servicios de pago.

También es necesario señalar que existe otra serie de disposiciones en el derecho español que son instrumentos idóneos para la regulación de p ago mediante tarjeta en el comercio electrónico: el TRLGDCU y la LRLOCM.

5.13. Consideraciones finales

Partiendo del análisis de los aspectos vistos en este capítulo llegamos a las siguientes conclusiones:

Guinea-Bissau no está totalmente preparada para establecer un sistema de pago mediante tarjeta en el comercio electrónico seguro teniendo en cuenta el diagnóstico alcanzado a través de la matriz DAFO, en la que se ha constatado la necesidad de crear un modelo que permita el desarrollo del comercio electrónico en Guinea-Bissau basado sobre todo en las variables claves que se han detectado.

La no existencia de un marco jurídico sobre el comercio electrónico en el país se debe sobre todo a l a falta de personal altamente capacitado en la materia, a la falta de cultura sobre el comercio electrónico y a la inexistencia de un gran volumen de negocios.

A nuestro juicio, para la implementación de un s istema de pago electrónico es necesario dotar al país de un cuerpo normativo obligatorio a nivel nacional, específico y concreto para las transacciones electrónicas y el pago mediante tarjeta en el comercio electrónico seguro, ya que es un requisito básico para la evolución de un sistema de pago electrónico. Por último, se ha de subrayar que el desarrollo del servicio de la sociedad de la

información y el comercio electrónico jugaría un papel fundamental en el crecimiento económico de Guinea para elevar el nivel cultural de la población[743].

De ahí la necesidad de proponer la aprobación de ciertas normas jurídicas semejantes a las existentes en España, basándose sobre todo en los análisis legislativos, doctrinales y jurisprudenciales que hemos hecho a lo largo de esta investigación. Una futura normativa jurídica sobre la protección de los consumidores y usuarios titulares de los medios de pago, al igual que el TRLGDCU, donde se recojan y regulan adecuadamente todas las cláusulas abusivas que pudieran tratar de imponer las entidades bancarias e incluyendo a los proveedores de acceso a Internet en los contratos firmados con los titulares de la tarjeta y los proveedores de bienes o servicios. En este sentido, el presente modelo puede convertirse en una herramienta eficaz para el desarrollo de Guinea-Bissau.

Somos conscientes de que la implementación de un modelo de comercio electrónico seguro en este país africano se enfrenta a algunos problemas relacionados con la falta de conciencia sobre el uso y las ventajas de las nuevas tecnologías de la información y la comunicación. Sin embargo, esto no es motivo para alegar su no aplicación.

Cabe subrayar que es necesario contar con un marco normativo sólido y coherente[744] que proteja a los sujetos intervinientes en la operativa de

[743] A nuestro juicio, para llegar a beneficiar de las oportunidades del comercio electrónico, el gobierno debe eliminar las debilidades existentes en cuanto a nivel de formación del capital humano, es decir, el gobierno guineano debe invertir en la educación y formación de profesionales y formular políticas apropiadas en materias de perfeccionamiento del capital humano, con el motivo de beneficiar del servicio de la sociedad de la información y el comercio electrónico.

[744] Según se prevé en el Informe de la Reunión de Expertos sobre Estrategias en Materia de Comercio Electrónico para el Desarrollo, celebrada en Ginebra, Suiza, entre el 10 y el 12 de julio de 2002, de que "la necesidad de una infraestructura jurídica y normativa que respalde y fortalezca las actividades del comercio electrónico constituye una de las principales cuestiones que los responsables de las políticas deberían abordar al definir una

pago mediante tarjeta en el comercio electrónico, donde aún se encuentran lagunas normativas que permiten la impunidad de bandas organizadas dedicadas a cometer fraudes en medios de pago electrónico. Para que el comercio electrónico en nuestro país se potencie, el marco legal que impulse y proteja el comercio electrónico entre empresa y consumidor debe dar garantías a los sujetos intervinientes de que sus derechos están protegidos.

Es imprescindible que el legislador guineano en el momento de redactar estas normas abogue por que las mismas sean redactadas en tal sentido, es decir, que contemplen no solo el pago mediante tarjeta de crédito sino, además, el pago por dispositivo móvil.

Finalmente, se ha de resaltar que la creación de unas infraestructuras tecnológicas y el mayor acceso a las mismas son requisitos indispensables para el desarrollo del comercio electrónico en Guinea-Bissau. Siguiendo la tesis sostenida por la OMC, "no puede haber comercio electrónico si no hay acceso a dos elementos infraestructurales indispensables. En primer lugar, para que la información pueda transmitirse, deben estar instalados el equipo y los programas necesarios. En segundo lugar, debe haber acceso a redes de comunicación".

estrategia en relación al comercio electrónico. La legislación correspondiente debería tener por finalidad proporcionar seguridad y neutralidad tecnología y comercial, así como las barreras que se oponen al acceso y utilización del comercio electrónico y a la libre circulación de este. Así pues, es indispensable garantizar que las transacciones en línea sean legalmente validas vinculantes y obligatorias" (TD/B/COM.3/47), 25/07/02, p. 13.

Universidad
Carlos III de Madrid

CONCLUSIONES

Conclusiones generales

1. Se diseñó un proyecto estratégico para la implementación del comercio electrónico en Guinea-Bissau, basado en el modelo propuesto que incorpora como aporte metodológico la utilización de una matriz DAFO, entre otros elementos. Además, se demuestra en el capítulo V que el logro de la transformación requerida descansa en factores internos.

2. Es importante destacar desde este punto de vista, que el presente diagnóstico reafirma la necesidad de aplicar de inmediato una estrategia adaptativa que posibilite la minimización de las debilidades a partir del aprovechamiento de las oportunidades que el entorno brinda al país, potenciando la apertura del comercio electrónico. Al mismo tiempo, se requiere de forma simultánea la aplicación de la estrategia ofensiva.

3. También queda demostrada que en nuestro país se evidencia la falta de cultura bancaria por una buena parte de la población, así como el bajo nivel de desarrollo de las nuevas tecnologías de la información y la comunicación, aspectos que pueden dificultar e impedir el desarrollo del comercio electrónico y el pago mediante tarjeta de crédito en Internet y la introducción de otras modalidades de medios de pago electrónico. No obstante se evidencia el esfuerzo de las autoridades del BCEAO y de las entidades bancarias para insertarse en las nuevas exigencias del comercio electrónico.

4. El actual cuadro legal y de infraestructuras del sistema de pago guineano se caracteriza por su inadecuación a las exigencias del

servicio de la sociedad de la información y el comercio electrónico. De ahí que creemos que el gobierno debe optar por la creación de un sistema de pago electrónico partiendo de iniciativas legislativas importantes que den soporte a la estructuración del referido sistema de pago guineano.

5. La matriz DAFO nos ha permitido estudiar principalmente las oportunidades y los retos para la futura implantación de comercio electrónico en Guinea-Bissau. Al mismo tiempo, se hizo análisis del sistema de pago electrónico en España, basado sobre todo en el pago mediante tarjeta en el comercio electrónico, se analizó la jurisprudencia así como las normativas que regulan cuestiones relacionadas con la seguridad en las operativas de pago mediante tarjeta: obligaciones, protección, y responsabilidades de los entes intervinientes en la operativa de pago mediante tarjeta en el comercio electrónico.

6. Finalmente, creemos que la implantación del comercio electrónico y el pago mediante tarjeta de crédito en Guinea-Bissau abrirán una nueva oportunidad de intercambio para los futuros proveedores de bienes o servicios y los consumidores. Por lo que su implementación debe estar orientada a garantizar la seguridad jurídica en las transacciones electrónicas. Además, debe estar inspirada en los principios universales del derecho del comercio electrónico.

7. Desde el punto de vista de la seguridad técnica, la implantación del comercio electrónico y el pago mediante tarjeta generan riesgos derivados de los problemas relacionados con los sistemas informáticos o electrónicos que sirven de instrumentos para el intercambio de mensajes de datos, los cuales son susceptibles de

usos, abusos y errores por personas no autorizadas que pueden provocar graves perjuicios. Dichos riesgos se producen especialmente cuando el comercio electrónico se desarrolla en Internet, siendo los más importantes:

a) La suplantación de la identidad del titular del mensaje
b) La alteración del mensaje durante la transmisión
c) La negativa de haberlo enviado o de recibido

8. Además de los problemas reseñados en los párrafos anteriores, se ha de resaltar que existen otros obstáculos que pueden dificultar la implantación del comercio electrónico y el pago mediante tarjeta de crédito en Guinea-Bissau:

   - Por ser uno de los países más pobres del mundo, su nivel de ingreso en la sociedad de la información es mínimo y la insuficiencia de acceso a Internet representa una más de sus carencias, junto con una infraestructura de comunicaciones muy deficiente.

   - La no existencia de unas infraestructuras básicas adecuadas, una logística bien definida, así como una estructura empresarial que sea capaz de aprovechar los rendimientos que se pueden obtener de la implantación del comercio electrónico en el país.

   - La baja tasa de bancarización. A nuestro juicio, solo se podrá conseguir una alta tasa de bancarización en el país cuando las entidades bancarias promuevan el uso del

dispositivo móvil como medio de pago alternativo a l a tarjeta de crédito.

Propuestas legislativas

Tras realizar esta investigación sobre la implantación del comercio electrónico y los medios de pago electrónicos en Guinea-Bissau, y habiendo formulado conclusiones generales, hemos de hacer llegar unas propuestas legislativas. En este sentido, cabe resaltar que existen una serie de problemas como el vacío jurídico de la legislación. A raíz de esta laguna jurídica existente, se propone la creación de tres normativas jurídicas:

Primero:

- Es imprescindible desarrollar una l ey de servicios de pag o electrónico que deberá incorporar un s istema común de derechos, obligaciones y responsabilidad para los sujetos intervinientes en la transacción electrónica u operativa de pago mediante tarjeta de crédito en el comercio electrónico.

- Dicha normativa deberá incluir preceptos relacionados con la protección de los consumidores y usuarios titulares de medios de pago electrónico en cuanto a uso fraudulento o indebido de la tarjeta de crédito en Internet

- Igualmente, es necesario regular de forma detallada en la misma normativa las cláusulas abusivas para detectarlas e imponer su no inclusión, regulando igualmente la responsabilidad de los sujetos intervinientes en el contrato de adhesión ante un posible fraude, no dejándolo, como venía sucediendo en el derecho español, a la voluntad de las partes.

En este sentido, resulta significativa la incorporación de la carga de prueba explicada en los capítulos III y IV de esta investigación.

Segundo:

- Destacar la necesidad de crear una normativa jurídica sobre firma electrónica para reforzar la confianza de los consumidores y usuarios titulares de la tarjeta, ya que la firma electrónica reconocida resulta ser un instrumento imprescindible para la comprobación de la procedencia e integridad de los datos intercambiados entre las partes intervinientes en la operativa de pago en Internet.

- Asimismo resulta especialmente destacable, a nuestro juicio, señalar que la utilización de la firma electrónica reconocida puede contribuir a atenuar las amenazas o riesgos en la operativa de pago en el comercio electrónico, especialmente en una red abierta como Internet. Por lo tanto, es necesario que el legislador guineano incluya en la ley obligaciones y responsabilidades de los prestadores de servicio de certificación.

Tercero:

- A nuestro juicio, es esencial para la implantación del comercio electrónico, la adopción de una ley de servicio de la sociedad de la información y comercio electrónico en Guinea-Bissau.

- El legislador guineano deberá ser lo más exhaustivo posible respecto a los actos que pueden ser considerados como servicios de la sociedad de la información y los que no son considerados como tal, así como aquellos actos que pueden

ser contrarios al Derecho, describiendo supuestos generales que sean capaces de incluir toda conducta de esta índole, evitando así las negativas consecuencias que origina la laguna legislativa al no recogerse determinados supuestos.

- Se deberán regular en la ley las diversas causas de responsabilidad de los proveedores de contenido y prestadores de servicios de intermediación. La incorporación legislativa de un cuerpo normativo de esta naturaleza en nuestro país es indispensable, dada la importancia que juega el comercio electrónico en la economía a nivel mundial.

- Se propone que el legislador incluya un inciso o apartado sobre aquellos prestadores que realizan actividades de alojamiento o de enlaces sin ánimo de lucro, es decir, sin recibir ningún tipo de remuneración ni directa ni indirecta vía publicidad. Ya que dichas actividades, al no tener carácter económico, quedan fuera del concepto de servicios de la sociedad de la información, y por tanto los artículos 14 a 17 de la LSSICE, en el caso de España no les son de aplicación. En este sentido, es fundamental proponerse y podría defenderse una extensión analógica de tales preceptos para cubrir las actividades no lucrativas o económicas.

- Se debe tener en cuenta de modo expreso la aplicabilidad de las exclusiones de responsabilidad a los supuestos de carácter gratuito.

- Es preciso que el legislador de la norma sobre comercio electrónico tenga en consideración no sólo su vital adecuación

al contexto del ordenamiento jurídico guineano, sino también que, por el avance vertiginoso de la sociedad de la información y el comercio electrónico, sea elaborada con una visión del futuro del país.

- Por último, queremos resaltar la necesidad de llevar a cabo modificaciones en el Código Civil con la intención de perfeccionar más su normativa en correspondencia con los requerimientos del comercio electrónico. Por lo que, se propone modificar el texto del art. 217.1 del Código Civil guineano, que debe quedar redactado de la siguiente manera: que la declaración o manifestación de voluntad: será expresa en su caso cuando la voluntad se manifiesta, verbalmente, por escrito, por medios electrónicos o cualquier otra tecnología.

- También, es imprescindible fijar el momento y el lugar de celebración de los contratos electrónicos, en el código civil y la Ley uniforme sobre derecho comercial de la OHADA.

Sugerencias

Tras realizar esta investigación sobre la implantación del comercio electrónico y los medios de pago electrónico en Guinea-Bissau, y habiéndonos formulado conclusiones generales así como propuestas legislativas, cabe efectuar las siguientes sugerencias:

1. El gobierno guineano debería introducir cursos de formación para los jueces, abogados, policías judiciales, y fiscales entre otros. Dichos cursos deben estar a cargo de profesores doctores especialistas en la materia.

2. Se deben organizar en el país cursos de maestrías y diplomaturas en Derecho del Comercio Electrónico, en las facultades de Derecho y Economía, lo que facilitará su conocimiento y difusión y permitirá que autores publiquen trabajos académicos y aplicativos. Además, debemos dejar constancia de la inexistencia de b ibliografías o trabajos de investigación relacionados con el derecho de la contratación electrónica.

3. Se debe celebrar un congreso internacional sobre la implantación del comercio electrónico y los medios de pago electrónico en Guinea-Bissau para permitir un estudio profundo sobre la materia, con participantes nacionales y extranjeros.

4. Se debe crear una Comisión que tendrá como objetivos fundamentales:

    - Proponer al Gobierno la política y las recomendaciones que impulsen el desarrollo del comercio electrónico en el país
    - Realizar actividades de divulgación que incrementen el conocimiento y la cultura sobre esta materia en el país
    - Identificar las medidas y regulaciones que deberán emitir los Organismos de la Administración Central del Estado para eliminar los obstáculos y crear las condiciones propicias para la implantación del comercio electrónico en Guinea-Bissau.
    - Identificar y patrocinar la realización de proyectos de comercio electrónico.

- Instrumentar las formas y vías adecuadas a fin de obtener y brindar cooperación internacional para el desarrollo del comercio electrónico

- Elaborar y proponer al Gobierno las líneas directrices de política sobre este tema en el plano internacional.

5. Por último, para resolver los pleitos existentes entre los entes intervinientes en la operativa de pago en el comercio electrónico, se propone la creación de una sala especializada en l os tribunales mercantiles para estos litigios.

Universidad
Carlos III de Madrid

BIBLIOGRAFÍA

BIBLIOGRAFÍA

ABASCAL ROJAS, Fco. *Como se hace un plan estratégico. Modelo de desarrollo de una empresa.* Pozuelo de A lcorcón (Madrid): ESIC Editorial, 1999.

--*El DAFO valora las debilidades, amenazas, fortalezas y oportunidades de la empresa.* [En línea] Disponible en Internet. http://www.barcelonanetactiva.com/barcelonanetactiva/images/es/2_El%20analisis%20DAFO_tcm106-22138.pdf(última consulta 5 de febrero de 2012).

ALAMILLO DOMINGO, I.; y URIOS APARISI, X. «Comentario crítico de la ley 59/2003, de 19 de diciembre, de firma electrónica», *Revista de la contratación electrónica*, núm. 46, 2004, pp. 3-64.

ALCOVER GARAU, G. «La firma electrónica como medio de prueba (valoración jurídica de los criptosistemas de c laves asimétricas)», *Cuadernos de Derecho y Comercio*, núm. 13, 1994, pp. 11 y ss.

--«El Real Decreto-Ley sobre firma electrónica», *RCE*, núm. 1, 2000, pp. 7 - 28.

--«Concepto de firma electrónica, firma electrónica y firma digital», en PERALES SANZ, J. L.: *La seguridad jurídica en las transacciones electrónicas. Seminario organizado por el Consejo General del Notariado en la UIMP.* Madrid: Civitas, 2002, p. 33.

--«*Introducción al Derecho Mercantil*». Madrid: Editorial Dilex, S.L., 2008.

ALEJANDRA MUCHART, M. ª *Contrato de cuenta corriente bancaria.* [En línea] disponible en Internet: http://www.buenastareas.com/ensayos/Contrato-De-Cuenta-Corriente-Bancaria/3055027.html (última consulta, 25 de noviembre de 2012).

ALONSO CONDE, A. B. *Comercio electrónico: antecedentes, fundamentos y estado actual.* Madrid: Dykinson, S.L., 2004.

ALONSO UREBA, A.; y ALCOVER GARAU, G. «La firma electrónica», en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J. M. (coords.). *Derecho de internet. Contratación electrónica y firma digital.* Prólogo de Ana Birulés I Bertrán. Elcano (Navarra): Aranzadi, 2000, pp. 175-20.

ALONSO SOTO, R.: "Tarjeta de crédito, medios de pago electrónico y derecho de la competencia", *en Estudios de Derecho Bancario Bursátil Homenaje a Evelio Verdera y Tuells*, t II. Madrid: La Ley, 1994, p.18.

ÁLVAREZ-CIENFUEGOS SUÁRES, J. M. ª. «La firma electrónica y el comercio electrónico en España. Comentario a l a legislación vigente», *Aranzadi,* diciembre de 2000.

ÁLVAREZ MARAÑON, G.; y PÉREZ GARCÍA, P. P. *Seguridad informática para empresas y particulares*. Prólogo de Juan Carlos G. Cuartango. Madrid: McGraw-Hill/ Interamericana, S.A., 2004.

ÁLVAREZ MARAÑON, G. «Seguridad en el comercio electrónico: ¿SSL o SET?» [En línea] disponible en Internet: http://www.iec.csic.es/criptonomicon/.../susurros08.htm(última consulta el 10 de mayo de 2012).

--«Compras seguras en la red», publicado en *PC Word digital*, el 1 de octubre de 2004[En línea] disponible en internet: http://www.idg.es/pcworld/Compras_seguras_en_la_Red/art161637.htm-74 (última consulta, el 10 de marzo de 2012).

--«*Medios de pago*». [En línea] Disponible en Internet: http://www.iec.csic.es/criptonomicon/comercio/cybercash.html-13k (última consulta el 5 de marzo de 2012).

---«SET a fondo Secure Electronic Transaction», en *La Revista de Tecnología y Estrategia de Negocio en Internet (RTENI*), núm. 22. Publicada el 12 de enero de 1999 [En línea] Disponible en Internet:http://www.idg.es/iWorld/articulo.asp?id=103068(última consulta, 12 de diciembre de 2012).

ALVARADO HERRERA, L. "La responsabilidad de los proveedores de servicios de pago en caso de no ejecución o ejecución defectuosa de operaciones en el proyecto de Ley de servicios de pago", en MADRID PARRA, A (dir.). *Derecho del sistema financiero y tecnología*. Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2010, p. 202.

--*La transferencia bancaria.* Madrid: Consejo Económico y Social, 1999.

ALVARENGA, J. «Potencialidades, política e programas de desenvolvimento económico em Guinea-Bissau», en *1ªs Jornadas de estudios sobre la cooperación para al desarrollo entre Europa y los países del área Sub-Sahariana, República Popular de Angola, República de Cabo Verde, República de Guinea Bissau, República Popular de Mozambique, Madrid, 28, 29, y 30 de septiembre de 1989.* Madrid*:* Editorial IEPALA, 1989, páginas: 1 carpeta.

ÁLVAREZ SÁNCHEZ, J. M. *La red como soporte de marketing y comunicación.* Vigo: Ideas Propias Editorial, 2005.

AMESTI MENDIZABAL, C.: "El concepto de contrato de apertura de crédito y su diferenciación respecto al contrato de préstamo", en S ÁNCHEZ CALERO, F. y CALERO-GUILARTE, J. (coords.). *Comentarios a Jurisprudencia de Derecho Bancario y Cambiario,* v II. *Consideraciones en entorno algunos aspectos de la cuenta corriente bancaria*. Madrid: 1993, p.70, nota. 4.

ANDREU MARTI, M. ª. M. «Consideraciones en entorno al pago con tarjetas electrónicas», en *Estudios sobre el Consumo*, núm. 33, 1995.

--*La protección del cliente bancario.* Prólogo de José Miguel Embid Irujo. Madrid: Tecnos, 1998.

APARICIO VAQUERO, J. P. "Los contratos electrónicos en el derecho español. El marco establecido por la Ley de servicios de la sociedad de la información y el comercio electrónico", MORO ALMARAZ, M. ª J. (dir.). *Internet y comercio electrónico*. Salamanca: Ediciones Universidad de Salamanca, 2003, pp. 177-216.

ARIAS POU, M. ª. *Manual práctico de comercio electrónico*. Madrid: La ley 2006.

--"Necesidad de seguridad en el comercio electrónico", en *Ciclo de Seminario Europeos contra el fraude en medios de pago. Retos y soluciones para los consumidores en el fraude en medios de pago,* celebrada de 11 a 12 de mayo. Barcelona. Zaragoza: ADICAE, 2009, p. 33.

ARISTOTELES MAGÁN PERALES, J. M. ª. «La nueva administración pública electrónica, las relaciones electrónicas entre la administración y el ciudadano. Especial referencia a la firma electrónica», en PUNZÓN MORALEDA, J (coord.). *Administraciones públicas y nuevas tecnologías.* Valladolid: Editorial Lex Nova, S.A., 2005, p.96.

AURIOLES MARTÍN, A. "Contratos bancarios", en JIMÉNES SÁNCHEZ, Guillermo J. (coord.). *Derecho mercantil*, 4. ª ed. Barcelona: Ariel, S.A., 1997, pp. 467-479.

AUGEL, J.; CARDOSO, C. *Transição Democrática na Guiné Bissau.* Bissau: INEP, 1996.

AAVV*. Diccionario básico jurídico*. Granada: Comares, 1993.

AZOFRA VEGAS, F. «La contratación electrónica bancaria», en *RDBB*, núm. 68, octubre- diciembre 1997, pp. 111 y ss.

BARRAL VIÑALS, I. "La seguridad en I nternet: La firma electrónica", en BARRAL VIÑALS, I (coord.). *La regulación del comercio electrónico. Totalmente adaptado a la LSSICE y a la modificación de la Ley del comercio minorista*. Madrid: Dykinson, S.L., 2003, p.83.

BARRIUSO RUIZ, C. *La contratación electrónica*, 3. ª ed. Madrid: Dykinson, 2006.

--*La contratación electrónica*. Madrid: Dykinson, 1998.

BARDAJÍ MUÑOZ, L. *Derecho mercantil. (Inspección de finanzas),* 4. ª ed., Madrid: Centro de Estudios Financieros, 1998.

BARUTEL MANAUT, C. *Las tarjetas de pago y crédito.* Barcelona: BOSCH, 1997.

--*El pago por medios electrónicos: una aproximación a las tarjetas*, Obra social y cultural de caja de Segovia, 2000.

BAUTECAS CALETRIO, A. *Pago con tarjeta de crédito. Naturaleza y régimen jurídico.* Navarra: Aranzadi, Monografía Asociada a la Revista Aranzadi de Derecho Patrimonial, núm. 15, 2005.

BELTRÁN SÁNCHEZ, E. M y ORDUÑA MORENO, J. Fco. (coords). *Curso de Derecho Privado*, 7. ª ed. Valencia: Tirant Lo Blanch, 2004.

Belt I. *Nuevas técnicas de fraude informático: el pharming.* Madrid, 01 de abril de 2 005 [En línea] Disponible en Internet: http://www.belt.es/noticias/2005/abril/01/pahrming.htm (última consulta 29 de octubre de 2012)

BERNAL JURADO, E. «Las tarjetas bancarias como mecanismos de pago en el comercio electrónico», en *Distribución y Consumo*, núm. 55, Diciembre 2000 -Enero 2001, pp. 67-74.

--*El mercado español de tarjetas de pago bancarias: situación actual y perspectivas*. Madrid: Civitas, 2001.

BERNAL JURADO, E. y PARRAS ROSA, Manuel. «El sistema de tarjetas de pago bancarios en España y su influencia en el desarrollo del comercio electrónico», en *Estudios sobre Consumo*, núm. 59, 2001, pp. 23-37.

BERCOVITZ RODRGÍUEZ-CANO, R. "Venta a distancia (Comentario al art. 46 LOCM)", en BERCOVITZ RODRÍGUEZ-CANO, R y LEGUINA VILLA, J (coords.). *Comentarios a las Leyes de ordenación del comercio minorista*. Madrid: Tecnos, 1997, pp. 727-729.

BERMEJO VERA, J. *El declive de la seguridad en el ordenamiento plural.* Cizur Menor (Navarra): Aranzadi, SA, 2005.

BIDGODI, H. *Electronic commer. Principles and practice.* San Diego (California): ACADEMIC PRESS, 2002.

BLANCO PÉREZ-RUBIO, L. «Las cláusulas abusivas en los contratos celebrados con consumidores: aplicación jurisprudencial de la Directiva 93/13», en *Separata de Revista Jurídica del Notariado (RJN)*, núm. 19 julio-septiembre 1996, pp. 206-208.

--«El control de contenido en condiciones generales y en cláusulas contractuales predispuestas», *en Separata de RJN* núm. 35 julio-septiembre 2000, pp. 9-36.

--"Cláusulas abusivas en la contratación electrónica", en BOTANA GARCÍA, G (coord.). *Comercio electrónico y protección de los consumidores*. Madrid: La Ley, 2001, pp. 510 y ss.

BOTANA GARCÍA, G. "Los contratos a distancia y la protección de los consumidores", en ILLESCAS ORTIZ, R (dir.). *Derecho del comercio electrónico*. Madrid: Editorial la Ley, 2001, pp. 347 y ss.

BOQUERA MATARREDONA, J. «El impago de la deuda por la entidad emisora de la tarjeta de crédito», en CUÑAT EDO, V. y BALLARÍN HERNÁNDEZ (dirs.). *Estudios sobre jurisprudencia bancaria*. Navarra, Aranzadi, 2000, pp. 387 y ss.

BROSETA PONT, M.; y MARTÍNEZ SANZ, F. *Manual de Derecho Mercantil, Contratos mercantiles derecho de los títulos valores. Derecho concursal,* 12. ª ed. Madrid: Tecnos, 2005.

--*Manual de Derecho Mercantil, Contratos mercantiles derecho de los títulos valores. Derecho concursal,* v II, 11ª. ed. Madrid: Tecnos, 2004.

--*Lecciones de Derecho Mercantil,* 13. ª ed*.* Madrid: Tecnos (Grupo Anaya, S.A.), 2009.

BRIZ, J.; y LASO, I. *Internet y comercio electrónico. Características, estrategias, desarrollo y aplicaciones*. Madrid: Coedición, ESIC Editorial y Mundi-Prensa, 2000.

BUSTO LAGO, J. M (coord.). *Reclamaciones de consumo. Derecho de consumo desde la perspectiva del consumidor*. Elcano (Navarra): Aranzadi, 2005.

BURGO PUYO, A. *El consumidor y los contratos en Internet.* Colombia: Universidad Externado de Colombia, 2007.

CABANILLAS SÁNCHEZ, A. *Las cargas del acreedor en el derecho civil y en el mercantil.* Madrid: Editorial Montecorvo, S.A., 1998

CACHÓN BLANCO, J. H. "El contrato bancario de apertura de crédito", en NIETO CAROL, U (dir). *Contratos bancarios& parabancarios.* Valladolid: Editorial Lex Nova, S.A., 1998, pp. 541- 568.

CAMPO, A.. *História da Guiné-Bissau em datas.* Lisboa: 2012.

CARDOSO, Carlos (s/d). *Os desafios da transição política na Guiné* Bissau. [En línea] Disponible en Internet: http://www.didinho.org/osdesafiosdatransicaopoliticanaguinebissau.htm (última consulta 12 de junio de 2012).

CARANCHO HERRERO, M. ª. T. “Breve apunte sobre la responsabilidad de los prestadores de servicios de intermediación”, en MURRILLO VILLAR, A.; y BELLO PAREDE, (coords.). *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*. Burgos (España): 2005, p. 202.

CARRASCOSA LÓPEZ, V.; POZO ARRANZ, Mª. A. y RODRÍGUEZ DE CASTRO, E. P. *La contratación informática: el nuevo horizonte contractual,* 3. ª. ed. Granada: Comares, 1999.

CARBONEL PINTANEL, J. C. *La protección del consumidor titular de las tarjetas de pago en la Comunidad Europea*. Madrid: Beramar, Colección de Estudios Internacionales, 1994.

CASELLAS, D. “obligaciones y responsabilidad excesiva para los usuarios”, en *Ciclo de seminarios europeos contra el fraude en medios de pago. Retos y soluciones para los consumidores en el fraude en medios de pago*. Zaragoza: ADICAE, 2009.

CASTAN TOBEÑAS, J.: *Derecho civil* español, *común y foral*, t. III. Madrid: Ed. Reus, 1978.

CASTELLANOS DE UBAO, L. G. E “Estudio de la Directiva y del Real Decreto-Ley de 17 d e septiembre de 1999 sobre firma electrónica”, en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords). *Derecho de internet. Contratación electrónica y firma digital*. Prólogo de Ana Birulés I Bertrán Elcano (Navarra): Aranzadi, 2000.

CASTILLEJÓ, E. M. “Eficacia jurídica de la firma electrónica”, en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital*. Prólogo de Ana Birulés I Bertrán. Elcano (Navarra): Aranzadi, 2000, pp. 261-278.

CASTILLEJO MANZANARES, R. *El juicio ejecutivo basado en pólizas bancarias.* Valencia: Tirant Lo Blanch, 1996.

CASTRO BROTTO, L. *Los sitios de comercio electrónico enfrentan nuevas amenazas*. [En línea] Disponible en Internet: http://la.trendmicro.com/la/about/news/pr/article/20081117164206.html(última consulta 25 de octubre de 2012).

CERVELLÓ GRANDE, J. M.; y FERNÁNDEZ, I. « La prueba y el documento electrónico», en MATEU DE ROS, R.; CENDOYA MÉNDEZ DE VIGO, J. M (coords.). *Derecho de Internet. Contratación electrónica y firma digital*. Prólogo de Ana Birulés I Bertran. Elcano (Navarra): Aranzadi, 2000, pp. 385- 406.

CHOMER, H. O. «La tarjeta de crédito y el derecho del consumidor. Algo más sobre la competencia de l os jueces que deben entender en el reclamo del saldo deudor», en *Revista de Responsabilidad Civil y Seguros*. Año 10, núm.2, 2008, pp. 1-5.

CLEMENTE MEORO, M. "La contratación electrónica", en *Incorporación de las nuevas tecnologías en el comercio: aspectos legales*. Publicación del Consejo General del Poder Judicial, núm. 71, 2005, pp. 157 y ss.

--"La contratación electrónica", en REYES LÓPEZ, María José (coord.). *Derecho de consumo*. 2. ª ed. Valencia: Tiran lo Blanch, 2002, p.192.

COLLS, M. *El dinero de plástico. Todo sobre las tarjetas de crédito*. Barcelona: Decálogo, 1990.

CORDEIRO, R. S. *Guiné-Bissau: entre as sombras do militarismo e da impunidade.* [En línea] Disponible en Internet: http://www.didinho.org/GUINEBISSAUENTREASSOMBRASDOMILITARISMOEDAIMPUNIDADE.pdf (última consulta 13 de junio de 2012).

*-Guiné-Bissau 1973-2005: uma relação civil-militar no processo de transição polític*a. [En línea] Disponible en Internet: http://www.didinho.org/GUINEBISSAUUMAANALISESOBREARELACAOCIVILMILITAR.pdf (última consulta, 12 de junio de 2012).

*-Dança de cadeira: Golpes de Estado entre Autoritarismo e a Democracia guineens*e[En línea] Disponible en Internet: http://www.didinho.org/Dancadecadeira.pdf (última consulta, 12 de junio de 2012).

-- *Guiné-Bissau: entre as sombras do militarismo e da impunidade.* [En línea] Disponible en Internet: http://www.didinho.org/GUINEBISSAUENTREASSOMBRASDOMILITARISMOEDAIMPUNIDADE.pdf(última consulta, 12 de junio de 2012).

COUTO CALVIÑO, R. *Servicios de certificación de firma electrónica y libre competencia.* Prólogo de, Ana Mª. Tobio Rivas. Granada: Comares, 2008.

CRUZ RIVERO, D. *Eficacia formal y probatoria de la firma electrónica.* Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2006.

--La firma electrónica reconocida. Análisis de los requisitos del art.3.3 de la ley 59/2003, de 19 de diciembre, de firma electrónica. Madrid: Consejo General del Notariado, 2006.

--"La atribución del riesgo de suplantación de identidad en la banca electrónica", en MADRID PARRA, A (dir.): *Derecho del sistema financiero y tecnología.* Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2010, pp. 237 y ss.

--«La suplantación de identidad en el ámbito electrónico y la defraudación de la banca electrónica», en *RDBB,* núm. 117, enero-marzo, de 2010, p.191- 227.

DAVARA RODRÍGUEZ, M. Á. *Las tarjetas electrónicas: algunas apreciaciones y jurisprudencia, Encuentro sobre informática y Derecho*. Madrid: 1997.

--*Manual de Derecho Informático*. Pamplona: Aranzadi, 1997.

--*La seguridad en las transacciones electrónicas: La firma electrónica.* Madrid: Universidad Pontificia Comillas de Madrid, 2005.

--*Manual de Derecho Informático.* Navarra: Aranzadi, S.A., 2004.

--«El comercio electrónico y los medios de pago», *ICADE, Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*, núm. 43, enero-abril, 1998, p.72.

DE ARRILLAGA, J. I., «La tarjeta de crédito», en *Revista de Derecho Público (RDP)*, núm. 65, septiembre, 1981, 784-804 p, especialmente pp.791y ss.

--«La apertura de crédito», *RDP*, Madrid, 1981, p.788.

DE CASTRO y BRAVO, F. « Las condiciones generales de los contratos y la eficacia de las leyes», *Anuario de Derecho Civil*, 1961, p. 297.

DE EIZAGUIRRE, J. Mª. *Cuenta corriente bancaria y clausula "sin gasto" en la STS de 7 de marzo de* 1974. San Sebastián: 1978.

DE MIGUEL ASENSIO, P. A., *Derecho privado de Internet*, 3. ª ed. Madrid: Civitas, 2002.

DELGADO K. C.; FERNÁNDEZ PANADERO, M. ª C. “Fundamentos de la world wide web. Nuevos formatos. Nuevos modelos de neg ocio”, en ILLESCAS ORTIZ, R (dir). *Derecho del comercio electrónico.* Madrid: Editorial la Ley, 2001, pp. 39 y ss.

DEVOTO, M. «La Economía Digital el dinero electrónico y el lavado de dinero», en *Revista de Derecho Informático,* núm. 001, agosto del 1998. [En línea] disponible en internet: http://www.alfa-redi.org/rdi-articulo.shtml?x=121(última consulta, el 12 de octubre de 2012).

DEL PESO NAVARRO, E. *Servicios de la sociedad de la información. Comercio electrónico y protección de datos*. Madrid: Ediciones Díaz de Santos, S.A., 2003.

DE QUINTO ZUMARAGA, Fco. *La firma electrónica. Marco legal y aplicaciones prácticas.* Barcelona: Difusión Jurídica y Temas de Actualidad, S.A., 2004.

DI MARCHI G. "Carte di credito e carte bancarie", en *Banca, Borsa e titoli di credito*, 1970-I, pp.321y ss.

DÍAZ, Gabriel; MUR, Fco; y SANCRISTÓBAL, E. *Seguridad en las comunicaciones y en la información*. Madrid: Universidad Nacional de Educación a Distancia, 2004.

DÍAZ MENDEZ, N. “Problemática procesal de l a ejecución del contrato de apertura de crédito”, en N IETO CAROL, Ubaldo (coord.). *Contratos Bancarios & Parabancarios*. Valladolid: Lex Nova, 1998, p. 575.

DÍAZ MORENO, A, «Concepto y eficacia de l a firma electrónica en l a Directiva 1999/93/CE, de 13 de diciembre de 1 999, por la que se

establece un marco comunitario para la firma electrónica», en *RCE,* núm. 2, febrero. Cádiz: EDICIP, 2000, pp. 3-52.

DÍAS PEREIRA, A. L. *Comercio electrónico na sociedade da informação: Da segurança técnica a segurança jurídica*. Coímbra: Livraria A lmedina, 1999.

DÍAZ VILCHES, F; y ALBAREDA FLORENSA, J. *Facturación telemática. Y sistema abierto de certificación electrónica acreditado por la ley.* Barcelona: Editorial Experiencia S.L., 2005.

DIEZ-PICAZO, L.; y GULLON, A. *Sistema de derecho civil. El contrato en general. La relación obligatoria*, vol. II, t. I. 12 ª ed. Madrid: Tecnos, 2012.

--*Sistema de derecho civil* vol. II, 6ª ed. Madrid: Tecnos, 1993.

--*Fundamentos del Derecho Civil Patrimonial,* Madrid: Civitas, 1996.

DOMÍGUEZ LUELMO, A. "Contratación electrónica con consumidores", en MATA y MARTIN, R. M (dir.). *Los medios electrónicos de pago. Problemas jurídicos.* Granada: Comares, 2007, pp. 66-166.

--"La contratación electrónica y la defensa del consumidor", en ECHEVARIA SAÉNZ, J. A (coord.). *El comercio electrónico*. Madrid: EDISOFER S.L., 2001, p. 34.

ELGUERO Y MERINO, J. M. ª «La técnica comercial de compra con tarjeta de crédito», *Tapia.* Publicación para el mundo del derecho, año VII, núm. 43, Diciembre de 1988, p.2.

ECHEBARRÍA SÁENZ, J. A. (coord.) *El comercio electrónico* Madrid: EDISOFER, S.L., 2001.

--«El dinero electrónico: construcción del régimen jurídico emisor-portador», en MATA Y MARTIN, Ricardo M. (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, pp. 219-267.

EMBID IRUJO, J. M. "La cuenta corriente bancaria", en N IETO CAROL, Ubaldo (dir). *Contratos bancarios y parabancarios*. Valladolid: Editorial Lex Nova, S.A., 1998, pp. 303-319.

ESCOBAR ESPINAR, M. *El comercio electrónico. Perspectiva presente y futura en España*. Madrid: Fundación Retevisión, 2000.

---*El comercio electrónico. Perspectiva presente y futura en España.* Madrid: Retvisión, 1999.

FARRANDO MIGUEL, I y CASTAÑER CODINA, J.:«Atribución y distribución de responsabilidad civil por uso no aut orizado de t arjetas», en *RDBB*, núm. 81, enero- marzo 2001, pp. 87-103.

FELIU ÁLVAREZ DE SOTOMAYOR, Silvia. *La contratación internacional por vía electrónica con participación de consumidores. La elección entre la vía judicial y la vía extrajudicial para la resolución de conflictos*. Granada: Comares, 2006.

FERNÁNDEZ-ALBOR BALTAR, Á. "Contratación electrónica en Internet", en GOMEZ SEGADE, José Antonio (dir.). *Comercio electrónico en Internet.* Madrid: Marcial Pons, 2001, pp. 299 y ss.

FERNÁNDEZ DOMINGO, J. I. "Algunas notas acerca de la contratación y el comercio electrónico", en ORDUÑA MORENO, Fco. J (dir.*). Contratación electrónica y comercio electrónico.* Valencia: Tirant Lo Blanch, 2003, p. 253.

FERNÁNDEZ JURADO, Y.; y VAQUERO LAFUENTE, M.ª E. *Las TIC y un desarrollo justo y responsable de los países en vías de desarrollo*. [En línea] Disponible Internet: http://www.eben-spain.org/docs/Papeles/X/sthr_Vaquro-buna.pdf(última consulta 12 de marzo de 2012).

FERNÁNDEZ LÓPEZ, J. M. «Tarjetas bancarias. Contratos bancario y financieros», en *Cuadernos de Derecho Judicial.* CGPJ, Madrid: 1993, pp. 202 y ss.

FERNÁNDEZ ORENES, F.; y VILLALOBO RUIZ, D. *La tarjeta de crédito, en Adarve corporación jurídica. Medios de pago. Toda la información indispensable para elegir el medio de pago más idóneo en sus relaciones comerciales.* Madrid: Fundación Confemetal, 2003.

FERNÁNDEZ-ARMESTO, J.; y DE CARLOS BELTRAN, L*. El Derecho del mercado financiero.* Madrid: 1992.

FERNÁNDEZ ENTRALGO, J. «Falsificación y utilización fraudulenta de tarjetas electrónicas. Tarjetas bancarias y Derecho penal», en *Cuaderno de Derecho judicial* vl (2002), p.58.

FERNÁNDEZ GARCÍA, E. M. y LÓPEZ MÓRENO, J. «La utilización indebida de tarjetas bancaria y EPROM en el Código penal de 1995: nuevos supuestos». Tarjeta bancarias y Derecho penal, en *Cuaderno de Derecho judicial vl* (2001), p.96.

FERNÁNDEZ GÓMEZ, Eva. *Conocimientos y aplicaciones tecnológicas para la dirección comercial*. Madrid: Editorial ESIC, 2004.

--*Comercio electrónico*. Madrid: McGraw-Hill/Interamericana de España S.A.U, 2006.

FERNÁNDEZ PANADERO, M. ª Carmen "Fundamentos de la Word wide web. Nuevos formatos. Nuevos modelos de negocio", en ILLESCAS ORTIZ, R (dir.). Derecho del comercio electrónico. Madrid: Editorial la Ley, 2001, pp. 39 y ss.

FERNÁNDEZ PÉREZ N. *El nuevo régimen de la contratación a distancia con consumidores. Especial referencia a la relativa a servicios financieros.* Getafe (Madrid): La Ley, 2009.

--*La contratación electrónica de servicios financieros*. Prólogo de L uis Fernández de la Gándara. Madrid: MARCIAL PONS, 2003.

FERRANDO VILLALBA, M. ª De Lourdes. "El contrato de tarjeta de crédito", en ORDUÑA MORENO, Fco. J; y TOMILLO URBINA, J. L. (dirs.). *Contratación bancaria*, t II. Valencia: Tirant Lo Blanch, 2001, pp. 81-351.

FERREIRA, M.; y NUMERIANO, R. *O que é golpe de Estado.* São Paulo: Brasiliense, 1993.

FISAS ARMENGOL, V. *Amílcar Cabral y la independencia de Guinea-Bissau*. Barcelona: Editorial Novas Terra, 1974.

FLORES DOÑA, M. ª S, *Impacto del comercio electrónico en el derecho de la contratación*. Madrid: Editoriales de Derechos Reunidos, S.A., 2002.

FONT, A. *Seguridad y certificación en el comercio electrónico. Aspectos generales y consideraciones estratégica*. Prólogo de A ndrés Pedreno Muñoz. Madrid: Fundación Retevisión, 2000.

FORCADA MIRANDA, Fco. J. "El registro de pr opiedad y las nuevas tecnologías. La publicidad formal. Acceso al proceso y efectos jurídicos", en ALMENAR BELENGUER, M.; y CARBONELL LLORENS, C.

Jurisdicción y registro de la propiedad y mercantil: nuevas áreas de interés común. Madrid: Consejo General de Poder Judicial, 2004, p.108.

FRAMIÑAN SANTAS, J. «Pagos en la red. Medios de pago on line a través de Internet», en GÓMEZ SEGADE, J. A. (dir.*). Comercio electrónico en Internet.* Madrid: Marcial Pons, 2001, pp. 373 y ss.

GALGANO, Fco. *Dritto commerciale. L`imprenditore. Imprensa. Contratti di imprensa. Titolo di credito. Fallimento,* 4ª, ed. Bolonia: Zanichelli, 1994.

GÁLLEGO HIGUERAS, G. F. «Comentario a la reciente Ley 59/2003, de 19 de diciembre de firma electrónica: algunas novedades al marco regulador», en *REDNT,* Aranzadi, núm. 12, 2006, p.30.

GARRIGUES, J. *Contratos bancarios*. 2. ª ed. Madrid: 1975.

GARCÍA MÁS, Fco. J. *Comercio y firma electrónicos. Análisis jurídico de los servicios de la sociedad de la información*. Valladolid: Edit. Lex Nova, 2001.

---*Autenticación y cifrado para un comercio electrónico*. [En Línea] Disponible en Internet: http://www.esegi.es (última consulta el 12 de noviembre de 2012).

--*Comercio y firma electrónicos. Análisis jurídico de los servicios de la sociedad de la información.* 2. ª ed. Valladolid: Edit. Lex Nova, 2004.

GARCÍA DEL POYO, R. "Aspectos mercantiles y fiscales del e-business", en ECHEVARIA SAÉNZ, J. A (coord.). *El comercio electrónico.* Madrid: Edisofer S.L., 2001, p. 491.

GARCÍA RODRÍGUEZ, A. «La L ey 16/2009, de 13 de noviembre, de servicios de pag o: transposición en España del régimen comunitario armonizado», en *RDBB,* núm. 117, enero-marzo 2010, pp. 273-278.

GARCÍA SANZAZ, A. «La retrocesión en el contrato de comercio electrónico», en MADRID PARRA, A (dir.). *Derecho patrimonial*. Prólogo de Manuel Olivencia. Madrid: Marcial Pons, 20007, pp.292 y ss.

GARCÍA SOLÉ, F. «Aspectos sobre la incidencia de la tecnología en el mercado de tarjeta», en *Instituto Católico de Administración y Dirección de Empresas (ICADE),* núm. 43 enero-abril, 1998, pp. 80 y ss

GARROTE FERNANDEZ-DIEZ, I.: «La responsabilidad civil extracontractual de los prestadores de servicios en línea por infracciones de los derechos de autor y conexo*», Revista de Propiedad Intelectual*, nº. 6, 2000, p. 43.

GETE–ALONSO Y CALERA, M. ª C. *Las tarjetas de crédito como medio de pago.* Madrid: Marcial Pons, 1997.

-*Las tarjetas de Crédito. Relaciones contractuales y conflictividad*. Madrid: Marcial Pons, 1997.

--*El pago mediante tarjetas de crédito*. Madrid: La Ley, 1990.

-«Las tarjetas como instrumento de pago», en DEL POZO CARASCOSA, Pedro y DÍAZ MUYOR, Manuel. *Contratación bancaria. (Jornadas celebradas en Tarragona el 6 y 7 de marzo de 1997. Universitat Rovira I Virgili)*. Madrid: Marcial Pons (Ediciones Jurídicas y Sociales), 1998, pp. 99 y ss.

GÓMEZ MENDOZA, M. ª "Consideraciones generales en torno a las tarjetas de crédito", en *Estudios en Homenaje a Joaquín Garrigues*, t II. Madrid 1971, pp. 391 y ss.

--«Tarjetas bancarias y cajeros automáticos», en NIETO CAROL, U (dir). *Contratos bancarios & Parabancarios*. Valladolid: Lex Nova, 1998, pp. 851-886.

--«Tarjetas bancarias», en GARCÍA VILLAVERDE, R.: *Contratos bancarios.* Madrid: 1992, pp. 363 y ss.

--*Tarjetas de crédito al consumo*. La ley, 1993.

-"La protección del titular de una tarjeta de crédito en Reino Unido, en *Estudios de Derecho Bancario y Bursátil. Homenaje a Evelio Verdera y Tuells"*, t II. Madrid: La Ley, 1994, pp. 1190 y ss.

--«Naturaleza de las tarjetas de crédito, sus clases y carga de la prueba en el supuesto de extradiciones en cajeros automáticos», en *RDBB,* núm. 54, abril-junio, 1994, pp. 489 y ss.

--«Recomendación de la UE 97/489, de 30 de julio de 1997, relativas a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular las relaciones entre emisor y titulares de tales instrumentos», en *RDBB*, núm. 69, enero- marzo, 1998, pp. 250 y ss.

--«Comercio electrónico y tarjetas de pago. (Comentario a las sentencias de la Audiencia Provincial de Cáceres de 28 de enero de 2004 y de la Audiencia Provincial de Barcelona del 22 de diciembre 2004)», en *RDBB,* núm. 99, julio-septiembre 2005, pp. 227 y ss.

GÓMEZ PORRÚA, J. «La tarjeta de crédito», en JIMÉNEZ SÁNCHEZ, G. J. (coord.), *Derecho mercantil*. 4. ª ed. Barcelona: Ariel S.A., 1997, p. 186.

GÓMEZ VIEITES, Á. *Enciclopedia de la seguridad informática.* Madrid: RA-MA, 2006.

GÓMEZ VIETES, Á; y VELOSO ESPIÑEIRA, M. *Economía digital y comercio electrónico.* Santiago de Compostela: EDITA Escuela de Negocios Caixa Nova-Torculo Edicións, S.L., 2002.

GONZÁLEZ GONZALO, A*. La formación del contrato tras la ley de servicios de la sociedad de la información y de comercio electrónico*. Granada: Comares, 2004.

GONZÁLEZ PACANOWSKA, I. "Condiciones generales y cláusulas abusivas", en BERCOVITIZ RODRÍGUEZ-CANO, R (dir.). *Comentario del texto refundido de la ley general para la defensa de los consumidores y usuarios y otras leyes complementarias. (Real Decreto Legislativo 1/2007).* Cizur Menor (Navarra): Aranzadi, SA, 2009, pp. 956 y ss.

GONZÁLEZ-MENESES, M. *La firma electrónica como instrumento de imputación jurídica.* Una reflexión de Derecho civil sobre la contratación electrónica, Madrid: Colegio Notarial de Madrid, 2010.

GRAMUNT FOMBUENA, Mª. D. "El estatuto jurídico de los prestadores de servicios de la sociedad de la información", en BARRAL VIÑAL, I (coord.). *La regulación del comercio electrónico.* Madrid: Dykinson, 2003, p. 17.

GROSS, M. *Los orígenes del modelo de análisis DOFA* (actualizado)[En línea] disponible en Internet: http://manuelgross.bligoo.com/content/view/455327/Los-origenes-del-modelo-de-analisis-DOFA-actualizado.html(última consulta 2 de noviembre de 2012).

GUARCH, C H. «Tarjetas», en LUNAS DÍAZ, M. ª J (dir.). *Asociación de Usuarios de Servicios Bancarios. AUSBANC Consumo. Malas prácticas bancarias*. Madrid: Formación AUSBANC, 2002, pp. 185 y ss.

GUASP, J*. Derecho.* Madrid: Edit. Ergos, 1971.

GUERRA B. J. T. «La conclusión de contratos por medios informáticos», en *Revista Informática y Derecho*, núm. 8, Mérida: Universidad Nacional de Educación a Distancia, Centro regional de Extremadura, 1995, pp. 63 - 131, especialmente p.114.

GUIJARRO COLOMA, L. «Fundamentos técnicos y operativos de la firma electrónica», en *Incorporación de las nuevas tecnologías en el comercio: aspectos legales*. Publicación del CGPJ, núm. 71, Madrid, 2006, pp. 229-258, especialmente pp.233-249.

GUIMARÃES, Mª R. «El pago mediante tarjetas de crédito en el comercio electrónico. Algunos problemas relativos a su naturaleza jurídica, marco contractual y régimen aplicable, desde una perspectiva comparada en los derechos portugués, español y comunitario», en MATA Y MARTIN, R M. (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, pp. 166-217.

--*As transferências electrónicas de fundos e os cartões de débito.* Coimbra: Almedina, 1999.

-- «Algumas reflexiões sobre o pagamento com cartão de crédito o débito no ámbito da contratação electrónica», em *Temas de Direito da informática e da Internet*. Coimbra: Editorial Coimbra, 2004, pp. 161-180.

--«Os cartões bancários e as cláusulas contratuais gerais na jurisprudencia portuguesa e española», em *Revista de Direito e de Estudos Sociais*, ano XLIII, núm. 1, Lisboa, 2002, pp. 55- 91.

GUISADO MORENO, Á. *Formación y perfección del contrato en Internet*. Prólogo de Leopoldo J. Porfirio Carpio. Madrid: Marcial Pons, Ediciones jurídicas y Sociales, S. A., 2004.

Guiné-Bissau: «Para Lá da Lei das Armas», *Briefing África* do Crisis Group N°61, 25 de J unho de 2009 . [En línea] disponible en I nternet http://www.crisisgroup.org/fr/regions/afrique/afrique-de-louest/guinee-bissau/B061-guinea-bissau-beyond-rule-of-thegun.aspx?alt_lang=pt (última consulta 2 de junio de 2012).

«Guinée-Bissau: besoin d'Etat», *Relatório África* do Crisis Group N°142, 2 de Julho de 2008[En línea] disponible en Internet: http://www.crisisgroup.org/fr/regions/afrique/afrique-de-louest/guinee-bissau/142-guinea-bissau-in-need-of-a-state.aspx(última consulta 2 de junio de 2012).

--«Para além dos compromisos: as perspectivas de r eforma na Guiné-Bissau», *Relatório África do Crisis Group*, núm. 183. Dakar, 23 de janeiro de 2012. [En línea] disponible en Internet: http://www.crisisgroup.org/fr/regions/afrique/afrique-de-louest/guinee-bissau/183-beyond-compromises-reform-prospects-in-guinea-bissau.aspx?alt_lang=pt(última consulta, 2 de junio de 2012).

Instituto nacional de estadística. *Situación geográfica* [En línea] disponible en Internet: http://www.stat-guinebissau.com/pais/index_quadro_fisico.htm(última consulta 18 de junio de 2012).

GUTIÉREZ, J.; IBEAS, Á. "Criptografía", en GUTIÉREZ, J.; y TENA, J. *Protocolos criptográficos y seguridad en redes*. Santander (Cantabria): Universidad de Cantabria, 2003, pp. 63 y ss.

HARGAIN, D. "Ejecución del contrato por medios electrónicos", en FERRER, A; HARGAIN, D; y CAFFERA, G (coords). *Comercio electrónico. Análisis jurídico multidisciplinario.* Buenos Aires: Euros Editores S.L., 2003, pp.161-17.

HERNÁNDEZ LAVADO, L. «Contratación electrónica», en PERALES SANZ, J. L (dir.). *La seguridad jurídica en las transacciones electrónicas. Seminario organizado por el Consejo General del Notariado en la UIMP.* Madrid: Civitas, 2002, p.153.

HERNANDO, I. *Contratos Informáticos. Derecho Informáticos. Legislación y práctica*. San Sebastián: Librería Carmelo, 1995.

HORTAL I VALLVÉ, J.; ROCCATAGLIATA, F. y VALENTE, P. *La fiscalidad del comercio electrónico*. Valencia: Editorial CISS, S.A., 2000.

IBAÑEZ, J., *El control de internet*. Madrid: La catarata, 2005.

ILLESCAS ORTIZ, R. *Derecho de la contratación electrónica*. 2ª ed. Madrid: Civitas, 2009.

--*Derecho de la contratación electrónica.* Madrid: Civitas, 2001.

--«las nuevas responsabilidades electrónicas legales y su aseguramiento», en *II Congreso sobre las Nuevas Tecnologías y sus repercusiones en el seguro: Internet, Biotecnología y Nanotecnología.* Barcelona, *17 y 18 de noviembre de 2011.* Madrid: AIDA, 2012, pp. 13-28.

--«Oferta, perfección y prueba del contrato electrónico», en *Nuevas formas contractuales y el incremento del endeudamiento familiar*, núm. 50, Madrid: Consejo General de Poder Judicial, 2004, pp. 239 y ss.

--«Contratación electrónica», en ILLESCAS ORTIZ, R. y VISCASILLAS PERALES, Pilar. *Derecho Mercantil internacional. El Derecho Uniforme*. Madrid: Editorial Centro de Estudios Ramón Areces, S.A., 2003.

--«La firma electrónica y el Real Decreto Ley 14/1999, de 17 de septiembre», en *Derecho de los Negocios*. Octubre, 1999, pp. 165-176.

--"Los principios de la contratación electrónica, revisitados", en MADRID PARRA, A; y GUERRERO LEBRÓN, M .J. (Coords.). *Derecho patrimonial y tecnología: revisión de la contratación electrónica con motivo del Convenio de las Naciones Unidas sobre Contratación electrónica de 23 de noviembre de 2005 y de las últimas novedades legislativas.* Madrid: Marcial Pons, 2007, pp. 21-38.

«El comercio electrónico: fundamentos de der echo y el principio de equivalencia funcional», en *Boletín de Inflación y Análisis Macroeconómico,* núm. 56, mayo 199, pp. 2913 y ss.

INFANTE PÉREZ, V. «Tarjeta de crédito: su estudio jurídico», *Boletín del Ilustre Colegio de Abogado de Madrid*, núm.6. Madrid: 1989, p.32.

INZA, J. "Banca electrónica. "Sistema de pagos avanzados", en ILLESCAS ORTÍZ, Rafael (dir.). *Derecho del comercio electrónico.* Madrid: La ley, 2001, pp. 260-267.

ITEANU, O. *Internet et le Droit. Aspects juridiques du commerce électronique.* Paris: Éditions Eyrolles, 1996.

JAVIER CORTÉS, L. «Los Contratos bancarios (II)», en MENÉNDEZ, Aurelio. *Lecciones de Derecho Mercantil*, 3. ª ed. Navarra: Aranzadi, S.A., 2005, pp. 676-677.

JAVIER, S.; y PRIOR, F. *La banca móvil como catalizador de la bancarización de los pobres: modelos de negocio y desafíos regulatorios.* [En línea] disponible en Internet: http: //www.redmicrofinanzas.cl/web/wp-content/uploads/2010/07/La-Banca-M%C3%B3vil-como-catalizadora-de-la-bancarizaci%C3%B3n-de-los-pobres.pdf(última consulta el 21 de noviembre de 2012).

JIMÉNEZ SÁNCHEZ, G.J (coord*.). Lecciones de Derecho Mercantil,* 7ª ed. Prólogo de M anuel Olivencia. Madrid: Tecnos (Grupo Anaya, S.A.), 2002.

--*Lecciones de Derecho Mercantil,* 13ª ed*.* Madrid: Tecnos (Grupo Anaya, S.A.), 2009.

---«Tarjeta de crédito», en MONTOYA MELGAR, A (dir). *Enciclopedia Jurídica Básica*, vol. IV. Madrid: 1995, pp. 6472-647.

---*Lecciones de derecho mercantil*, 10. ª ed. Madrid: Tecnos, 2005.

JESÚS MILLÁN T. R. «El pago por móvil empieza a des pegar», en *Comunicaciones Word*, núm. 181, 2003. [En línea] disponible en Internet: http://www.networkworld.es/El-pago-por-movil-empieza-a-despegar/seccion-analisis/articulo-151153 (última consulta el 11 de noviembre de 2012).

JULIA BARCELÓ, R. *Comercio electrónico entre empresarios*. *La formación y prueba del contrato electrónico (EDI).* Valencia: Tirant Lo Blanch, 2000.

KABUNDA BADI, M. «Relaciones internacionales africanas y relaciones interafricanas en la era de l a globalización», en E CHART MUÑOZ, E (coord.). *África en el horizonte. Introducción a la realidad socioeconómica del África subsahariana*. Madrid: Catarata, 2006, pp. 82 y ss.

KOUDAWO, F.; MENDY, P. K. *Pluralismo político na Guiné-Bissau:* uma transição em curso. Bissau: INEP, 1996.

LAFUENTE SÁNCHEZ, R. *Los servicios financieros bancarios electrónicos.* Valencia: Tiran lo Blanch, 2005.

--«Análisis de l a Ley 59/2003, de firma electrónica, tras dos años de vigencia; problemas no resueltos en torno a los certificados de firma electrónica», en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 11. Madrid: 2006, pp. 39-54.

LASARTE ÁLVAREZ, C. *Manual sobre protección de consumidores y usuarios*, 2. ª ed., revisada y actualizada. Madrid: Dykinson, S.L. 2005.

LARA NAVARRA, P y MARTINEZ USERO, J. Á. Comercio electrónico: la fidelización del usuario. FUOC. Publicada: marzo de 20 03 [En línea] Disponible en Internet: http://www.uoc.edu/dt/20168/-119k-(última consulta el 6 de febrero de 2012).

LEGAZ LACAMBRA, L. *Filosofía del Derecho*. 2. ª ed. Madrid: 1961; GUASP, Jaime*. Derecho.* Madrid: Edit. Ergos, 1971.

LINARES ANDRADE, L. "La ejecución y preferencia de las pólizas bancarias de préstamo y apertura de c rédito", en CUÑAT EDO, V; y BALLARIN HERNANDEZ, R. *Estudios sobre jurisprudencia bancaria*. Navarra: Aranzadi S.A., 2000, p. 251.

LLANEZA GONZÁLEZ, P. *Internet y comunicaciones digitales. Régimen legal de las tecnologías de la información y la comunicación*. Barcelona: Bosch, 2000.

LÓPEZ JIMENÉZ, J. M. *Comentario a la ley de servicios de pago.* Madrid: BOSH, S.A., 2011.

--*Uso ilícito de las tarjetas bancarias.* Barcelona: BOSCH, S.A., 2009.

LOMASCOLO SZITTYAY, R. “Aspectos técnicos de la firma electrónica”, en *las Jornadas sobre Firma digital y Administraciones Públicas,* celebrada en el Instituto Nacional de Administración Públicas (INAP), de 8 a 9 de junio de 2002. Madrid: INAP, 2003, pp. 29-78.

LÓPEZ PASCUAL, J y SEBASTIAN GONZÁLEZ, A. *Gestión bancaria. Factores claves en un entorno competitivo.* 3. ª ed. Madrid: McGraw-Hill/Interamericana de España, S.A.U, 2007.

LÓPEZ DE PRADO, R. «Bibliotecas de museos en España: características específicas y análisis DAFO», en *Revista General de Inform*e José. «Tarjetas de crédito: su estudio jurídico», en *Boletín del Ilustre colegio de Abogado de Madrid. Revista Jurídica General,* núm. 6, 1989, p. 47-63.

MADRID PARRA, A.: «Seguridad en el comercio electrónico», en ORDUÑA MORENO, F.J (coord.). *Contratación y comercio electrónico.* Valencia: Tirant lo Blanch, 2002, pp. 148-151.

--«Impulso al empleo de técnicas electrónicas», en SÁNCHEZ CALERO, F. y SÁNCHEZ-CALERO GUILARTE, Juan (coords.). *Comentario a la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero*. Elcano (Navarra): Aranzadi, 2003, pp. 803 y ss.

--«Dinero Electrónico: reflexiones sobre su calificación jurídica», en MADRID PARRA, A (dir). *Derecho del sistema financiero y tecnología*. Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2010, pp.17-60.

--«Dinero Electrónico: reflexiones sobre su calificación jurídica», en *RDBB*, núm. 116, octubre-diciembre 2009, pp. 9 y ss.

--«El convenio de N aciones Unidas sobre contratación electrónica», en MADRID PARRA, A (dir.). *Derecho patrimonial y tecnología*. Prólogo de Manuel Olivencia. Madrid: MARCIAL PONS, 2007, pp. 39.-113.

--«Seguridad, pago y entrega en el comercio electrónico», en *RDM*, núm. 241, 2001.

--«La contratación electrónica», en *Estudios en Homenaje a Aurelio Menéndez*, t III. Madrid: Civitas, 1996.

MANUEL VIILLAR, J. «Una aproximación a la firma electrónica», en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital*. Prólogo de Anna Birulés I Bertrán. Elcano (Navarra): Aranzadi, S.A., 2000, p. 170.

MARIEL FERRARI, R. *Macroeconomía. Teoría del crecimiento y el desarrollo*. [En línea]Disponible en Internet: http://www.monografias.com/trabajos32/teoria-crecimiento/teoria-crecimiento.shtml (última consulta el 31 de octubre de 2012).

MARIMÓN DURÁ, R. *La tutela del usuario en el contrato bancario electrónico.* Monografía asociada a R evista Aranzadi de D erecho y Nuevas Tecnologías, núm. 8. Cizur Menor (Navarra): Aranzadi, S.A., 2010.

MARIÑO LÓPEZ, A. *Responsabilidad contractual por utilización indebida de tarjeta de crédito*. Prólogo de GETE-ALONSO y CALERA, Mª. C. Buenos Aires: Abeledo-Perrot, Lexis Nexis, S.A., 2004.

--*Uso fraudulento de tarjetas de crédito por terceros no autorizados. Daños y responsabilidad civil*. Madrid: Marcial Pons, 2006.

---*Responsabilidad contractual por utilización indebida de tarjeta de crédito*. Tesis Doctoral presentada en la Facultad de Derecho. Departamento de Derecho Privado. Universidad Autónoma de Barcelona, 2003.

MARÍN LÓPEZ, J. J. *La venta a distancia, en Nueva ordenación del comercio minorista en España.* Madrid: Cámara de Comercio e Industria de Madrid, 1996.

MARÍO GOFFAN, C. *Tarjetas de Crédito. Análisis contractual, problemática procesal y penal.* Buenos Aire: Abeledo-Perrot, 2000.

MARTÍNEZ-CAÑABATE, J. R., «El contrato de emisión de tarjeta de crédito bancaria», en *Revista General del Derecho,* núm. 567, Madrid, diciembre de 1991.

MARTÍNEZ NADAL A.˙L. *Comercio electrónico, firma digital y autoridad de certificación*. Prólogo de Guillermo Alcover G. Madrid: Civitas, 1998.

--*Comentarios a la Ley 59/2003, sobre firma electrónica*. Madrid: Aranzadi, 2004.

--*El dinero electrónico. Aproximación Jurídica*. Madrid: Civitas S.L., 2003.

--«Medios de pago en el comercio electrónico», en *Actualidad Informática Aranzadi,* octubre 2000, pp. 1 y ss.

--«La firma electrónica como equivalente funcional, espejismo o realidad», en PERALES SANZ, J. L (dir.). *La seguridad jurídica en las transacciones electrónicas. Seminario organizado por el Consejo General del Notariado en la UIMP.* Madrid: Civitas, 2002, p.185.

--«La Ley española de firma electrónica (Real Decreto Ley 14/1999)», en ILLESCAS ORTIZ, R. (dir.). *Derecho del comercio electrónico*. Las Rozas, 2001, pp.77 116.

--«El pago con tarjeta en la contratación electrónica. En general art. 46 LOCM», en *RDBB,* núm. 84, octubre-diciembre 2001, pp. 27 y ss.

--"Atribución de responsabilidad al comerciante o a la entidad bancaria proveedora del sistema de pago en caso de uso fraudulento de tarjetas en el comercio electrónico", en M ADRID PARRA, A. (dir.). *Derecho patrimonial y tecnología*. Prólogo de Manuel Olivencia Madrid: Marcial Pons, 2007, pp. 213-232.

--"La Firma Electrónica en el Derecho Español", en MORO ALMARAZ, M. ª Jesús (dir.). *Internet y comercio electrónico II y III jornada sobre Derecho Informático (2ª 2001. Salamanca, España).* Salamanca: Ediciones Universidad de salamanca, 2003, pp. 113 y ss.

MARTÍNEZ NADAL, A.P. y FERRER GOMILA, J. L. Aproximación al Concepto Jurídico de Dinero Electrónico. Ponencia presentada en el *Segundo Congreso de Comercio Electrónico CSE '03*, celebrado Universitat de les Illes Balears, en junio de 2003, Barcelona. [En línea] Disponible en Internet:http://www.criptored.upm.es/guiateoria/gt_m081e.htm-4k(última consulta 24 de diciembre de 2012).

MARTÍNEZ GONZÁLEZ, M. «Mecanismo de seguridad en el pago electrónico», en MATA y MARTIN, Ricardo M. (dir.). *Los medios electrónicos de pago. Problemas jurídicos.* Granada: Comares, 2007, pp. 6 y ss.

MARTÍNEZ LÓPEZ, L; MATA MATA, Fco.; y BERNAL JURADO, E. *Medios de pago electrónico. Piedra angular en el desarrollo del comercio electrónico.* [En Línea] Disponible en Internet: http://150.214.178.8/sinbad2/files/publicaciones/77.pdf.(última consulta el 17 de agosto de 2012).

MARTÍNEZ ROSADO, J. « La Ley 44/2006, de 29 de diciembre, de mejorada de la protección de los consumidores y usuarios: contenido y reflexiones a la luz de su articulado», en *RDBB,* núm. 106, mayo-junio 2007, pp. 136 y ss.

MARTÍNEZ SALAZAR BASCUÑANA, L. *Condiciones generales y cláusulas abusivas en los contratos bancarios.* Cádiz: Editora de P ublicaciones Científicas y Profesionales, S.L., 2002.

MARTÍNEZ-SIMANCAS, J. "Contratos bancarios e Internet", en MATEU DE ROS, Rafael y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital.* Prólogo de Ana Birulés I Bertrán. Elcano (Navarra): Aranzadi, S.A., 2000, p. 491.

MARTOS, J. J. *Defraudación fiscal y nuevas tecnologías*. Cizur Menor (Navarra): Aranzadi, SA., 2007.

MARQUÉS, J. R.; LAGO, Pilar y GONZÁLEZ, Carmen. *Medios de pago*. *Guía del usuario*. Madrid: Ediciones Pirámide, 1999.

MATA y MARTIN, R. M. «Medios electrónicos de pago y delitos de estafa», en MATA y MARTIN, R. M. (dir.). *Los medios electrónicos de pago. Problemas jurídicos*. Granada: Comares, 2007, pp. 319- 365.

MATEO HERNÁNDEZ, J. L. *El Dinero Electrónico en Internet. Aspectos técnicos y jurídicos.* Granada: Comares, 2005.

MATEU DE ROS, R. "Principios de la contratación electrónica en la Ley de servicios de la sociedad de la información y el comercio electrónico", en MATEU DE ROS, R.; y GALLEGO, M. López-Monís (coords). *Derecho de Internet. La Ley de servicios de la sociedad de la información y de comercio electrónico*. Prólogo de Carlos López Blanco. Cizur Menor (Navarra): Aranzadi, S.A., 2003, pp. 71-104.

MÉNDEZ VILLAR, M. «La tarjeta de crédito en España», *Banca española*, núm.43, 1973, pp. 57 y ss.

MÉNDEZ GONZÁLEZ, F.P. «La firma electrónica y registro: consideraciones generales», en *Revista Electrónica de Derecho y Nuevas Tecnologías, Aranzadi,* núm. 12, 2006, pp. 17 y ss.

MENDONÇA, J. A. *La tasa de bancarización en Guinea-Bissau sube un 0,2% en seis meses.* [En línea] disponible en Internet: http://www.agareso.org/es/actualidad/mundo/guinea-bissau-cronicas-de-baba/item/443-a-taxa-de-bancarización-en-guinea-bissau-sube-un-02-en-seis-meses(última consulta el 3 de noviembre de 2012).

MOLL DE MIGUEL, S. *El contrato de cuenta corriente. Una concepción unitaria de sus diferentes tipos*. Bilbao: 1977.

MOLLE, G.; y DISEDERIO, L. *Manuale di Diritto bancario e dell`intermediazione finanziaria,* 5ª ed. Milán: Guiffrè, 1997.

MOLES PLAZA, R. J.: *Derecho y control en Internet. La reusabilidad de Internet*. Barcelona: Ariel, 2004.

MOLEJON ULLOA, R. «Los medios de pago electrónicos. Limitaciones en su uso», *RED*I: *Alfa-redi*, núm. 101, diciembre de 2006, pp. 5-6. [En Línea], disponible en Internet. http://www.alfa-redi.org/rdi-articulo.shmt.(última consulta el 2 de enero de 2012).

MORENO NAVARRETE, M. Á. *Derecho-e. Derecho del comercio electrónico.* Madrid: Marcial Pons, 2002.

--*Contratos electrónicos*. Madrid: Marcial Pons, 1999.

MONTES RODRÍGUEZ, Mª. P. "Las condiciones generales de los contratos bancarios y la protección de los consumidores y usuarios", en CUÑAT EDO, Vicente y BALLARÍN HERNÁNDEZ, R (coords.). *Estudios sobre jurisprudencia bancaria*. Elcano (Navarra): Aranzadi, S.A., 2000, p.108.

MUGUILLO, R. A. *Tarjeta de crédito. Régimen legal. Doctrina. Jurisprudencia.* Prólogo de F ernando M. Macheroni. Buenos Aries: Editorial Asterea, 1988.

MUÑOZ MUÑOZ, R. «Criptografía», en RUBIO VELÁZQUEZ, R; RODRÍGUEZ SAU, C.; y MUÑOZ MUÑOZ, R. *La firma electrónica. Aspectos legales y técnicos*. Barcelona: Ediciones Experiencia, S.L., 2004, p.179.

NAVARRO CHINCHILLA, J. J. Condiciones generales y cláusulas abusivas en la contratación bancaria, en NIETO CAROL, U. (dir.). *Condiciones generales de la contratación y cláusulas abusivas.* Valladolid: Lex Novas, 2000, p. 548.

NORES GONZÁLEZ, C. M. en el que se desenvuelve la firma electrónica en la Administración General del Estado, *en las Jornadas sobre «Firma digital y Administraciones Públicas»,* celebrada en el Instituto Nacional de Administración Públicas (INAP), de 8 a 9 de junio de 2002. Madrid: INAP, 2003, pp.15-28.

NUÑEZ LOZANO, P.L. *Tarjeta de crédito*. Madrid: Consejo Económico y Social, 1997.

NÚÑEZ-LAGOS, Fco. *Contratos bancarios*. Madrid: Centro de Formación del Banco de España, 1995.

ORICH, J. M. *Análisis de FODA* [En línea] disponible en Internet http://manuelgross.bligoo.com/content/view/284581/Guia_para_el_analisisFODA.htm (última consulta 2 de noviembre de 2012).

ORTEGA DÍAZ, J. Fco. *La firma y el contrato de certificación electrónicos*. Prólogo de Eduardo Galán Corona. Madrid: Aranzadi, SA, 2008.

ORMAZABAL SÁNCHEZ, G. «La prueba mediante documento electrónico digitalmente firmado», *Actualidad Civil*, 1999.

-«El valor probatorio de la firma electrónica», en PEGUERA POCH, M. *Derecho y nuevas tecnologías*. Barcelona: Editorial UOC, 2005.

-La prueba documental y los medios e instrumentos idóneos para reproducir imágenes, sonidos o archivar y conocer datos. Madrid: 2000.

PACHECO CAÑETE, M.: «La protección del consumidor una vez perfecto el contrato en las ventas de productos a distancia a través de Internet», *La Ley*, núm. 15184, 15 noviembre 2000, p. 3.

PANIZA FULLANA, A. *Contratación a distancia y defensa de los consumidores. Su regulación tras la reforma de la Ley de Ordenación de Comercio minorista y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Granada: Comares, 2003.

PARDO, F. "Implantación social. Situación del comercio electrónico en España", en GÓMEZ SEGADE, José Antonio (dir.). *Comercio electrónico en Internet*. Madrid: Marcial Pons, pp. 91 y ss.

PARDO LÓPEZ, J. *Condiciones generales y cláusulas contractuales predispuestas. La Ley de condiciones de la contratación.* Prólogo de Juan Ignacio Font Galán. Madrid: Marcial Pons, Ediciones Jurídicas y Sociales, S.A., 1999.

--«La Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación», en *DRAVIDIAN,* núm. 95. p. 325-384.

PARDO GATO, J. R. *Las páginas web como soporte de condiciones generales contractuales*. Navarra: Aranzadi, S.A., 2003.

--las cláusulas abusivas en los contratos de adhesión (Análisis legislativo y jurisprudencial). Madrid: DIJUSA, S.L., 2004.

PASTOR SEMPERE, M.ª C. *Dinero electrónico*. Prólogo de Luis Fernández de la Gándara. Madrid: Editoriales de Derecho Reunidas, S. A., 2003.

PASQUAU LIAÑO, M. "Las ventas especiales. Ventas a distancia (Comentario a los artículos 38 a 48)", en PIÑAR MAÑAS, José Luis y BELTRÁN SÁNCHEZ, Emilio (dirs.). *Comentarios a la Ley de ordenación del comercio minorista y la Ley orgánica complementaria.* Madrid: Civitas, 1997, p. 352.

PATRONI VIZQUERRA, U. El pago electrónico, en Revista del Derecho Informático. [En Línea], disponible en Internet. http://www.alfa-redi.org/rdi-articulo.shmt(última consulta el 2 de enero de 2012).

PAYERAS CAPELLA, M. "Los servidores de acceso y alojamiento: descripción técnica y legal", en CAVANILLAS MÚGICA, S (coord.). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*. Granada: Comares, 2005, p. 22.

PECES-BARBA, G. *Curso de derechos fundamentales,* vol. I. Madrid: Eudema, 1991.

PÉREZ SERRABONA GONZÁLEZ, J. L.; FERNÁNDEZ FERNÁNDEZ, L. M. *La tarjeta de crédito. Derecho comunitario europeo. Doctrina y formularios.* Granada: Comares: 1993.

--*La tarjeta de crédito: hacia un estatuto jurídico*. Granada: Edit. TAT, 1987.

PÉREZ GIL, J. «La prueba del pago por medios electrónicos», en M. MATA Y MARTIN, R (dir.). *Los medios electrónicos de pago. Problemas jurídicos.* Granada: Comares, 2007, pp. 383-410.

--«Documento Informático y firma electrónica: aspectos probatorios», en ECHEBARRÍA SÁENZ, J. A. (coord.). *El comercio electrónico* Madrid: Editorial Edisofer, S.L., 2001, pp. 222 y ss.

PÉREZ RODRÍGUEZ, Á. Mª. "La responsabilidad por phishing en la banca electrónica. (Notas a propósito de la sentencia de primera instancia de Castellón de 25 de junio de 2008)", en MADRID PARRA, Agustín (dir.). *Derecho del sistema financiero y tecnología.* Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2010, pp. 209-234.

PERALES VISCASILLAS, M.ª P. "Formación del contrato electrónico", en *Régimen Jurídico de Internet*. CREMADES, J.; FERNÁNDEZ-ORDÓÑEZ, M.A.; en ILLESCAS ORTIZ, R. (coords.). Madrid: La Ley, 2002, pp. 408-409.

PETIT LAVALL, M. ª V. *La protección del consumidor de crédito: las condiciones abusivas de crédito.* Valencia: Tirant Lo Blanch, 1996.

PETIT LAVALL, Mª. V.; y JUAN Y MATEU, F. “Cláusulas abusivas en los contratos bancarios”, en MENÉNDEZ MENÉNDEZ, A; y DÍEZ-PICAZO, Luis (dir). *Comentarios a la ley sobre condiciones generales de la contratación.* Madrid: Civitas, S.L., 2002, p. 1368.

PLAZA PENADÉS, J. «Contratación electrónica y pago electrónico. (En el derecho nacional e internacional)», en ORDUÑA MORENO, Francisco J. (dir.). *Contratación y comercio electrónico*. Valencia: Tirant Lo Blanch, 2003, pp. 451-475.

--«Firma electrónica, registro mercantil y sociedades. La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», en ORDUÑA MORENO, Fco J. (dir.). *Contratación y comercio electrónico.* Valencia: Tirant Lo Blanch, 2003, pp. 489- 526.

--«Firma electrónica, registro mercantil y sociedades. “Firma electrónica, y su regulación en el Derecho español”», en ORDUÑA MORENO, Fco. J. (dir.). *Contratación y comercio electrónico*. Valencia: Tirant Lo Blanch, 2003, pp.531- 574.

--“Cuestión de Derecho privado”, en PLAZA PENADÉS, J. (coord.). *Cuestiones actuales de derecho y tecnologías de la información y la comunicación (TICS). Monografía asociado a Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 4. Cizur Menor (Navarra): Aranzadi, S.A., 2006, p. 219.

---“Responsabilidad civil de los intermediarios en Internet”, en GARCÍA MEXIA, P (dir.). *Principios de derecho de Internet*, Valencia: Tirant lo blanch, 2005, pp. 399- 400.

«El pago a través de Redes de Comunicación en el Derecho Español y Comunitario», *REDI*, núm. 23, junio 2000. [En línea] disponible en Internet: http://www.vlex.com/redi. (última consulta, 20 de marzo de 2012).

PUZON MORALEDA, J.; y SÁNCHEZ RODRÍGUEZ, Fco. «Reflexión en torno al documento electrónico y la firma electrónica» en *Diario La Ley* nº 6986, Año XXIX, de 10 de julio de 2008, ref. D.217, pp. 1646 y ss.

RAMIÓ AGUIRRE, J. «La seguridad informática y sus amenazas», en SOLER MATUTES, Pere (dir.). *Manual de gestión y contratación Informática. Comentarios, jurisprudencia actualizada y formularios de contratos, modelos oficiales del COEIC*. Navarra: Aranzadi, SA., 2006, p. 153.

RAMOS HERRANZ, I.; y VILLAGOMEZ RODIL, A. (dirs.). *Contratos mercantiles especiales.* Madrid: Consejo general de poder judicial, 1997.

--«Tarjetas electrónica: problema de nuevo cuño y continuidad de los corte clásico», en VILLAGOMEZ RODIL, A (dir.). *Contratos mercantiles especiales.* Madrid: Consejo General del Poder Judicial, 1997, pp. 419-495.

--«Cheques electrónicos», en *RDM,* núm. 229, julio-septiembre de 1998, pp. 1223-1249.

--«Medios de pago electrónico», en BOTANA GARCÍA, G. A. (coord.). *Comercio electrónico y protección de los consumidores*. Madrid: La Ley, 2001, pp. 555 y ss.

RAMOS SUAREZ, F. «Eficacia Jurídica de una transacción electrónica. La Figura del No Repudio», en la *REDI*, núm. 12, julio 1999 [En línea] Disponible en Internet: http://www.alfa-redi.org/rdi_artículo.shtml?x=300 (última consulta 2 de diciembre de 2012).

--«Protocolo SET», *REDI,* núm. 3, octubre de 1998.

--«Seguridad en la venta de un producto por Internet», en la *REDI,* núm. 4, de noviembre de 1998[En línea] Disponible en Internet: http://www.alfa-redi.org.(última consulta, 2 de diciembre de 2012).

--*El comercio electrónico: la seguridad técnica y jurídica*. [En Línea] Disponible en Internet: http://www.masterdisseny.com/master-net/legalia/0006.php3(última consulta, 6 de julio de 2012).

REYES LÓPEZ, M. J. "Los métodos comerciales. La ley de ordenación del comercio minorista", en REYES LÓPEZ, M. J (coord.). *Derecho de consumo*. 2. ª ed. Valencia: Tirant lo Blanch, 2002, p.170.

RIBAS ALEJANDRO, J. «Riesgo legales en Internet. Especial referencia a la protección de datos personales», en MATEU DE ROS, R.; y CENDOYA MÉNENDEZ DE VIGO, J. M. (coords.). *Derecho de internet. Contratación electrónica y firma digital*. Prólogo de Anna Birulés I Bertrán. Elcano (Navarra): Aranzadi, S.A., 2000, p.147.

--*Aspectos jurídicos del comercio electrónico en Internet,* 2. ª ed. Navarra: Aranzadi S.A., 2001.

RICO CARRILLO, M. *Comercio electrónico. Internet y Derecho*, 2. ª ed. Venezuela: LEGIS, 2005.

--«Dinero electrónico», en *RCE*, núm. 31, octubre, 2002, pp. 3 y ss.

--«El pago mediante tarjeta en el comercio electrónico a través de Internet», *RC-E*, núm. 3, marzo de 2000, p.4.

--«Firma electrónica», *Conferencia impartida en el Curso del Doctorado en Derecho, programa general*. Getafe: Universidad Carlos III de Madrid, 27 de enero de 2006.

--«Responsabilidad civil de los intermediarios derivada del pago con tarjetas en el comercio electrónico a t ravés de Internet». *REDI,* núm. 017 diciembre 1999, pp.1-10.

--"Responsabilidad civil de los intermediarios derivada del pago con tarjetas en el comercio electrónico a través de internet", en *RDI*, núm. 017, diciembre del 1999, pp. 1 a 10[En Línea] disponible en Internet: http://www.alfa-redi.org/rdi-articulo.shtml?x=385 (última consulta, 4 de febrero de 2012).

--La protección de los consumidores en las transacciones electrónicas de pago, en *Telematique*, vol. 6, núm. 003, 2007, Universidad Rafael Belloso Chacin. Zulia (Venezuela), pp. 33 a 49. [En línea] disponible en Internet: http://redalyc.uaemex.mx/pdf/784/78460303.pdf (última consulta 12 de septiembre de 2012).

--«La protección de los consumidores en las transacciones electrónicas de pago», en *Primera Revista Multimedia Científica de Estudios Telemáticos en Venezuela* vol. 6, núm. 3, 2007 [En Línea] Disponible enInternet:http://www.publicaciones.urbe.edu/index.php/telematique/article/view/835/2043(Última consulta, 4 de julio de 2012).

RIVERO ALEMÁN, S. *Crédito, Consumo y Consumo Electrónico. Aspectos jurídicos bancarios.* Navarra: Aranzadi, 2002.

--*Disciplina del crédito bancario y protección del consumidor. (Cap. V. El crédito y el uso de medios electrónicos*). Pamplona: Aranzadi, 1995.

RIBÓN DURÁN, L. *El Diccionario de Derecho. Los conceptos del Derecho positivo, con sus variedades terminológicas en la América hispana y con referencias a la sistemática del Derecho civil, mercantil, constitucional, administrativo, fiscal, laboral, penal, comunitario y procesales*. Barcelona: Bosch, Casa Editorial, S.A., 1987.

ROBLES, S. «Seguridad en redes y protección criptográfica de la información», en *II Congreso sobre las Nuevas Tecnologías y sus repercusiones en el seguro: Internet, Biotecnología y Nanotecnología.* Barcelona, *17 y 18 de noviembre de 2011.* Madrid: SEAIDA, 2012, pp. 77-96, especialmente pp. 77-96.

RODRÍGUEZ ADRADOS, A. *Firma electrónica y documento electrónico*. Madrid: Consejo General Del Notariado, 2004.

--«La Firma electrónica», en *RDP*, diciembre 2000, pp. 927 y ss.

ROMEO CASABONA, C, «La utilización abusiva de las tarjeta de crédito», en *RDBB,* 1987, núm. 26, pp. 303 y ss.

ROMERO JUNQUERA, A. «La arquitectura de paz y seguridad africana. Un compromiso de la Unión Europea», en *La importancia geoestratégica del África subsahariana.* Centro Superior de Estudios de la Defensa Nacional (España): Editorial, Ministerio de Defensa, Secretaría General Técnica, 2010, p. 165.

RODRÍGUEZ DE LAS HERAS BALLELL, T. *El régimen jurídico de los mercados electrónicos cerrados (e-Marketplaces*. Prólogo de Rafael Illescas Ortiz. Madrid: Marcial Pons, 2006.

---"El reparto de riesgo y la atribución de responsabilidad en el uso de tarjeta en la contratación electrónica", en RICO CARRILLO, M. (coord.) *Derecho de las Nuevas Tecnologías,* Buenos Aires: La Roca, 2007, pp.322 y ss.

---«La responsabilidad por *software* defectuoso en la contratación mercantil», en *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 10, 2006, pp. 83-110.

---«El tercero de confianza en el suministro de información. Propuesta de un modelo contractual para la sociedad de la información», en *Anuario de Derecho Civil,* Tomo LXIII, Fascículo III, 2010, pp. 1245-1284.

---«Terms of Use, Browse-Wrap Agreements and Technological Architecture: Spotting Possible Sources of Unconscionability in the Digital Era», en *Contratto e Impresa. Europa,* 2/2009, Luglio-Dicembre, Anno XIV, pp. 849-869.

---«Intermediación en la Red y responsabilidad civil. Sobre la aplicación de las reglas generales de la responsabilidad a las actividades de intermediación en la Red», en *Revista Española de Seguros,* núm. 142, 2010, pp. 217-259.

---también publicado en VV.AA., *I Congreso sobre las Nuevas Tecnologías y sus repercusiones en el seguro: Internet, Biotecnología y Nanotecnología,* Madrid: Fundación Mapfre, 2011, pp. 13-50.

---«Las agencias de rating como terceros de confianza: responsabilidad civil extracontractual y protección de la seguridad del tráfico», en *RDBB,* núm. 120, octubre-diciembre 2010, pp. 141-177.

---"La formación del contrato en el entorno electrónico y los procedimientos electrónicos de contratación", en CALVO CARAVACA, A L.;

CARRASCOSA GONZÁLEZ, J (coords.). *Estudios sobre contratación internacional,* Madrid: Colex, 2006, pp. 535-572.

---"Las condiciones de uso de los sitios *web* y los *browse-wrap agreements*", en CALVO CARAVACA, A. L.; OVIEDO ALBÁN, J (coords.), *Nueva Lex Mercatoria y contratos internacionales.* Bogotá: Ediciones Jurídicas Gustavo Ibáñez, 2006, pp. 305-346.

---"Las condiciones de uso de los sitios web y los browse-wrap agreements", en *Derecho del Comercio Internacional – temas y actualidades (DeCita),* núm. 5/6, 2006, pp. 43-73.

RODRIGO GONZÁLEZ, O. *Comercio electrónico*. Madrid: Edit. Anaya Multimedia (Grupo Anaya, S.A.), 2008.

--«Recomendación de la Comisión de la CEE en relación con las tarjetas de crédito», en *RDBB*, 1987, núm. 28, pp. 903 y ss.

ROBLES ELEZ-VILLAROEL, J. F. *Practicas incorrectas y condiciones abusivas en las operaciones Bancarias*. Madrid: Instituto Superior de Técnicas y Prácticas Bancarias. S.L., 1994.

RODRÍGUEZ RUIZ DE VILLA, D. "La prestación de los servicios de certificación", en HUERTA VIESCA, Mª. I.; y RODRÍGUEZ RUIZ DE VILLA, D. *Los prestadores de servicios de certificación en la contratación electrónica*. Prólogo de F ernando Sánchez Calero. Navarra: Aranzadi, S.A., 2001, pp. 57-66.

ROBLES POMPA, J (coord.). *Práctica y Normalización Del Sistema y los Medios de Pago*, 2. ª ed. Madrid: Instituto superior de técnicas y prácticas bancarias, 2002.

ROMEO MARTINEZ-CAÑABATE, J., «El contrato de emisión de tarjeta de crédito bancaria», en *RGD*, núm. 567, Madrid, diciembre de 1992.

ROSSELLÓ MORENO, R. *El comercio electrónico y la protección de los consumidores*. Barcelona: Cedecs Editorial S.L., 2001.

RUIZ-GALLARDÓN, M. "Fe pública y contratación telemática" en MATEU DE ROS, R. y CENDOYA MÉNENDEZ DE VIGO, J.M. (coords.). *Derecho de internet. Contratación electrónica y firma digital*. Prólogo de Anna Birulés I Bertrán. Elcano (Navarra): Aranzadi, S.A., 2000, p.105.

RUIZ MUÑOZ, M. "El uso fraudulento de tarjetas de pago en la Directiva 2007/65/CE: La obligación de notificación y reclamación del usuario", en BOSH CAPDEVILA, E (dir.). *Derecho contractual Europeo. Problemas, propuestas y perspectivas.* Barcelona: Bosch, 2009, p.125.

--«Tutela de los consumidores en el electrónico», en *RCE*, núm. 90, 2008, pp. 3-90.

RUIZ, L. R. «Uso ilícito y falsificación de tarjetas bancarias». Revista de Internet, Derecho y Política. núm.3, UOC. 2006, [En línea]. Disponible en internet: http://www.uoc.edu/idp/3/dt/esp/ruiz.pdf (última consulta 15 de agosto de 2012).

SALAZAR BASCUÑANA, L. M. *Condiciones generales y cláusulas abusivas en los contratos bancarios.* Cádiz: Editora de Publicaciones Científicas y Profesionales, S, L., 2002.

SABATER BAYLE, E. «Cuatro principios sobre tarjetas electrónicas en los textos comunitarios», en H uarte de San Juan (*Revista Derecho de la Facultad. de Ciencias Humanas y Sociales. Derecho*,), núm. 1, 1994.

SÁNCHEZ CALERO, F. *Instituciones de Derecho Mercantil*, vol II, 24. ª ed. Madrid: MacGraw-Hill, 2002.

--*Instituciones de Derecho Mercantil*, T II. Títulos-valores, contratos mercantiles, Derecho concursal y marítimo, 22 ª ed. Madrid: McGraw Hill, 1999.

--«Contrato de cuenta corriente mercantil y el de cuenta corriente bancaria y rendición de cuenta», en *RDBB,* núm. 1992, pp. 545-546.

SÁNCHEZ-CALERIO GUILARTE, J. «En torno a la responsabilidad del titular de una tarjeta de crédito cuando la compañía que gestiona las tarjetas de crédito resulta insolvente», en *RDBB*, núm. 28, 1987, pp. 903 y ss.

--«La Armonización comunitaria de los sistema de pago electrónicos (tarjeta)». *Noticias de la CEE*, Madrid, 1989, año 5, núm. 58.

--«Recomendación relativa a los sistemas de pago y tarjeta de crédito», en *RDBB*, núm. 32, 1988, pp. 942 y ss.

--«Tarjeta de crédito y tutela del consumidor», en *RDBB*, núm. 98, abril-junio, 2005, pp. 204 y ss.

SANCHIS CRESPO, C.; y CHAVELI DONET, E. *La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000 (doctrina jurisprudencia y formularios)*. Valencia: Tirant lo Blanch, 2002.

--*La prueba por soportes Informáticos*. Valencia: Tiran Lo Blanch, 1999.

--«La prueba por soporte informáticos en la LECiv 1/2000», en *AI A,* núm. 36, julio de 2000.

SÁNCHEZ GÓMEZ, A. *El sistema de tarjeta de crédito*. Granada: Comares, 2006.

--"Comentario del art. 106 TRLGDCU, sobre pago mediante tarjeta", en BERCOVITZ RODRÍGUEZ-CANO, R (*Comentario del texto refundido de la ley general para la defensa de los consumidores y usuarios y otras leyes complementarias*. Cizur Menor (Navarra): Aranzadi, 2009, p. 1320.

--«Proyecto de C ódigo bancario relacionado con los sistemas de pag o electrónico», en *RDBB*, núm. 37, enero- marzo 1990, pp. 211 y ss.

SANJUÁN y MUÑOS, E. «Las condiciones generales de la contratación y el comercio electrónico», en *incorporación de las nuevas tecnologías en el comercio: aspectos legales,* Estudios de Derecho Judicial, núm. 71, CGPJ, Madrid, 2006, p. 32.

SÁNCHEZ NAVARRO, E. «África subsahariana. Sus recursos y desarrollo», *en La importancia geoestratégica del África subsahariana.* Centro Superior de Estudios de l a Defensa Nacional (España): Editorial, Ministerio de Defensa, Secretaría General Técnica, 2010 p. 265.

SCHILLACI, M. *Como tener éxito con su tienda virtual. Guía práctica de comercio electrónico*. Barcelona: INFORBOOK, S, S.L., 2009.

SEOANE BALADO, E. *La nueva era del comercio electrónico. Las TIC al servicio de la gestión empresarial*. Vigo: Editorial Ideas Propias, 2005.

SERRA RODRÍGUEZ, A. "Condiciones generales de la contratación y cláusulas abusivas en los contratos celebrados con consumidores", en REYES LÓPEZ, M. ª J (coord.). *Derecho privado de consumo*. Valencia: Tiran Lo Blanch, 2005, pp. 340 y ss.

--*Cláusulas abusivas en la contratación. En especial, las cláusulas limitativas de responsabilidad*. 2. ª ed. Cizur menor (Navarra): Aranzadi, SA., 2002, p. 76.

SPADA, P. "*Carte di credito: terza generazione' dei mezzi di pagamento", Le operazioni bancarie (a cura di Giuseppe PORTALE),* Milano: 1978.

S. STIGLITZ, R. y A. STIGLITZ, G. *Contratos por adhesión, cláusulas abusivas y protección al consumidor.* Buenos Aires: Depalma, 1985.

TEIXEIRA, R. *Tiro na democracia: uma análise sobre o processo de transição democrática na Guiné-Bissau,1994-2007*. [En línea] Disponible en Internet: http://www.didinho.org.(última consulta 12 de junio de 2012).

TRIAS DE BES, X. A. «E l pago electrónico», en RICCIUTO, Vicenzo (coord.). *Il contratto telematico e i pagamenti elettronici. L`esperienza italiana e spagnola a confronto*. Milano: Etitore Dott. A. Giuffre, 2004, pp. 55 y ss.

URÍA, R. *Derecho mercantil*. 28. ª ed. Madrid: Marcial Pons, 2002.

VÁZQUEZ CALLAO, E; y BERROCAL COLMENAREJO, J. *Comercio electrónico. Material para Análisis*. Madrid: Centro de p ublicaciones, Secretaria General Técnica, Ministerio de Fomento, 2000.

VÁZQUEZ RUANO, T. “La seguridad electrónica en la fase precontractual. Un apunte desde el derecho comunitario”, en MADRID PARRA, A. (dir.). *Derecho patrimonial y tecnología*. Madrid: Marcial Pons, 2007, pp. 250-274.

VEGA VEGA, J. A. *Contratos electrónicos y protección de los consumidores*. Madrid: Reus, S.A., 2005.

VELCHES TRASSIERA, A. J. *Aproximación a la sociedad de la información: firma digital, comercio y banca electrónica*. Madrid: Centro de Estudios Registrales, 20002.

VICENTE BLANCO, D. J. "Medios electrónico de pago y jurisprudencia competente en supuestos de Contratos Transfronterizos en Europa (Los criterios de competencia judicial del derecho comunitario europeo y su aplicación a las relaciones contractuales involucradas en los medios electrónicos de pago)", en MATA Y MARTÍN, R. M (dir.). *Los medios electrónicos de pago. Problemas jurídicos.* Granada: Comares, 2007, pp. 270-279.

VICENTE CHULÍA, Fco. *Compendio critico de Derecho Mercantil*, 2ª ed. t II. Barcelona: Bosch, 1986.

--*Introducción al Derecho Mercantil.* 17. ª ed. Valencia: Tiran lo Blanch, 2004.

-- *Introducción al Derecho Mercantil.* 19. ª ed. Valencia: Tiran lo Blanch, 2006.

VICÉNT, E. C.; y ALANDETE, T. B. *Aspectos jurídicos de los contratos atípicos*. I. 4ª ed. Barcelona*: Librería Bosch*, 1999.

VILATA MENADAS, S. "Condiciones generales de la contratación y el artículo 10 bis de la LGDCU", en *Protección de particulares frente a las malas prácticas bancarias II.* Publicación del Consejo General del Poder Judicial, núm. 79, 2006, pp. 52 y ss.

VILA SOBRINO, J. A. «Fundamentos técnicos. Aspectos técnicos para el desarrollo de aplicaciones de comercio electrónico», en GOMÉZ SEGADE, J.A (dir.). *Comercio en Internet*. Madrid: Marcial Pons, 2001, p.57.

ZAGANI, R. *Firma digitale e sicureza giuridica*. Casa Editrice Dott. Antonio Milani (CEDAM), 2000.

ZUMARÁN, S*. Contratación electrónica.* [En línea] disponible en Internet:http://pttcontraelmundo.files.wordpress.com/2007/10/la-contratacion-electronica-corregido.pdf (última consulta, 26 de agosto de 2012).

WRITER, S. *África ya es el segundo mayor mercado de móviles.* [En línea] disponible en I nternet: http://www.afrol.com/es/articulos/37755(última consulta, 23 de junio de 2012).

Universidad
Carlos III de Madrid

JURISPRUDENCIA ESPAÑOLA

JURISPRUDENCIA ESPAÑOLA

1. Sentencias del Tribunal Supremo

STS de 27 de mayo de 1966.

STS (Sala 2ª.), de 22 de noviembre de 1976.

STS 21 de noviembre de 1997.

STS (Sala1ª), de 16 de diciembre de 2009

2. Sentencias de Audiencias Provinciales

SAP de Zaragoza de 28 de abril de 1982.

SAP de Bilbao de 19 de diciembre de 1986.

SAP de Sevilla (sala 1ª) de 13 de diciembre de 1988.

SAP de Pamplona, de 18 de abril de 1989.

SAP de Barcelona (Sección. 16. ª), de 14 de septiembre de 1990.

SAP de Barcelona (Sección. 12. ª), de 17 de enero de 1992.

SAP de Alicante de 18 de enero de 1993.

SAP de Barcelona (Sección 12ª), de 14 de mayo de 1993.

SAP de Ciudad Real (Sección. 2. ª), de 20 de mayo de 1993.

SAP de Málaga (Sección 4ª), de 9 de septiembre de 1994

SAP de Valencia (Sección.2ª.), de 10 de octubre de 1994.

SAP Alicante de 30 de enero de 1995.

SAP de Baleares (Sección 5. ª), de 26 de febrero de 1997.

SAP de Barcelona (Sección 17ª), de 4 de noviembre de 1997.

SAP de Asturias de 8 de mayo de 1998.

SAP de Castellón (Sección 1. ª), de 26 de octubre de 1998.

SAP Barcelona (sección 17ª), de 25 de enero de 1999.

SAP de Navarra, de 20 de enero de 1999.

SAP de Palencia de 3 de febrero de 1999.

SAP de Madrid de 8 de abril de 1999.

SAP de Baleares de 25 de junio de 1999.

SAP de Toledo de 1 julio de 1999.

SAP de Málaga (Sección 4. ª), de 7 de mayo 2001.

SAP de Asturias, de 31 de julio de 200.1

SAP de Sevilla, de 4 de octubre de 2001.

SAP de Sevilla (Sección 6. ª), de 30 de julio de 2002.

SAP de Asturias (Sección 5ª), de 18 marzo de 2002.

SAP Cáceres, de 31 de enero de 2003.

SAP Asturias, de 13 de marzo de 2003.

SAP de Baleares (Sección 5ª), de 20 de marzo de 2003.

SAP de Bilbao (sección 1ª), de 22 de septiembre de 2003.

SAP de Castellón, de 5 de noviembre de 2003.

SAP de Baleares, de 17 de noviembre de 2003.

SAP de Madrid (Sección 8ª), de 28 de noviembre de 2003.

SAP de Barcelona (Sección 17ª), de 27 de febrero de 2004.

.SAP de Madrid (Sección 11ª), de 23 de abril de 2004.

SAP de Baleares (Sección 3ª), de 28 de mayo de 2004.

SAP de Madrid (Sección 21. ª), de 22 de junio de 2004

SAP de Murcia, de 29 septiembre 2004.

SAP de Barcelona (Sección19ª), de 27 de octubre de 2004.

SAP de Madrid, de 5 de noviembre de 2004.

SAP Madrid (sección 8ª), de 8 de noviembre de 2004.

SAP de Barcelona (Sección 1. ª), de 22 de diciembre de 2004.

SAP de Tarragona (Sección3ª), de 27 de diciembre de 2004.

SAP Castellón (Sección 1ª) de 30 de diciembre de 2004.

SAP de Sevilla (Sección 6. ª), de 31 de enero de 2005.

SAP de Madrid (Sección 13ª), de 11 de febrero de 2005.

SAP de Asturias (Sección 7ª), de 15 de febrero de 2005.

SAP de Asturias (Sección 6ª), de 14 de marzo de 2005.

SAP de Zaragoza de 12 de abril de 2005.

SAP de Bilbao (sección 5ª), de 28 de abril de 2005.

SAP de la de Guipúzcoa (Sección 3ª) de 31 de mayo de 2005.

SAP de Madrid, de 5 mayo 2005.

SAP de Madrid (Sección 13ª), de 11 de mayo de 2005.

SAP de Girona (Sección 1ª), de 9 de junio de 2005.

SAP de Pontevedra (Sección 1ª), de 29 de julio de 2005.

SAP de Tarragona (Sección 1ª) de 30 marzo de 2006.

SAP de la Coruña (sección 5ª), de 25 de abril de 2006

SAP de Madrid (Sección 14ª), de 25 de abril 2006.

SAP Valencia (Sección 9ª), de 17 mayo de 2006.

SAP de Murcia (Sección 3ª), de 13 julio de 2006.

SAP de Las Palmas (Sección 4ª), de 17 de julio de 2006.

SAP de Valencia (Sección 9ª), de 20 de julio de 2006.

SAP de Almería (Sección 3ª), de 15 septiembre de 2006.

SAP de Madrid (Sección 11. ª), de 3 de octubre de 2006.

SAP de Álava (Sección 2ª), de 6 de octubre de 2006.

SAP de Islas Baleares (Sección 3ª), de 13 de marzo de 2007.

SAP de Jaén (sección 1ª), de 20 de marzo de 2007.

SAP de Islas Baleares, de 24 mayo de 2007.

SAP Islas Baleares (Sección 5ª), de 10 octubre de 2007.

SAP de Pontevedra (Sección 1ª), de 19 de septiembre de 2007.

SAP de Navarra (Sección 1ª), de 8 de noviembre de 2007.

SAP de Soria (Sección 1ª), de 21 enero de 2008.

SAP de Madrid (Sección 14ª), de 6 de Febrero 2008.

SAP de Madrid (Sección 12ª), de 4 marzo de 2008.

SAP de Navarra (Sección 3ª), de 19 junio de 2008.

SAP de Alicante (Sección 8ª), de 17 julio de 2008.

SAP de Barcelona (Sección 16. ª), de 14 octubre de 2008.

SAP de Pontevedra (Sección 1. ª), de 25 de octubre de 2008.

SAP de Pontevedra (Sección 1ª), de 15 de octubre de 2008.

SAP de Sevilla (Sección 5ª), de 14 noviembre de 2008.

SAP de Granada (Sección 3ª), de 5 febrero de 2010.

SAP de Barcelona (Sección 1ª), de 4 de mayo de 2010.

1. Sentencias de los Juzgados provinciales

SJPI núm. 44, de Madrid, de 24 de septiembre de 2003.

SJPI núm. 7, de Guipúzcoa, Donostia-San Sebastián, 13 de octubre de 2004.

SJPI núm. 2, de Castellón, de 25 de junio de 2008.

SJPI núm. 9, de Valladolid, de 10 de marzo de 2009.

Universidad
Carlos III de Madrid

NORMATIVA ESPAÑOLA

NORMATIVA ESPAÑOLA

❖ *Leyes y Real Decretos leyes*

1. Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero (BOE, núm. 281, de 23 de noviembre de 2001), que viene a actualizar el marco establecido en la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista (*BOE*, núm. 15, de 15 enero de 1996).

2. Ley 47/2002, de 19 de diciembre, de reforma de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista (LOCM), para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE, en materia de contratos a distancia, y para la adaptación de la ley a diversas directivas comunitarias (*BOE*, núm. 304, de 20 de diciembre de 2002, p. 44759).

3. Ley 7/ 1995, de 23 de marzo, de Crédito al Consumo, (*BOE,* núm. 72, de 25 de marzo de 1995).

4. Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación (*BOE,* núm. 89, de 14 de abril de 1998).

5. Real Decreto Ley 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley general para la defensa de los

consumidores usuarios y otras leyes complementarias, que actualiza la Ley 26/1984, de 19 de julio de 1984. (Publicado, en *BOE*, núm. 287 de 30 de noviembre de 2007, pp. 49181-49215. Entrada en vigor: 01/12/2007; correcciones de errores en *B.O.E,* núm. 38/2008, publicada 13/02/2008, pp. 07730-07730).

6. Ley 59/2003, 19 de diciembre, de firma electrónica *(*Publicado, en *B.O.E*, núm. 30, de 20 de diciembre de 2003).

7. Real Decreto-Ley 14/1999, de 17 de septiembre de 1999 (Publicado, en *B.O.E,* núm. 224, de 18 de septiembre de 1999).

8. Ley de Enjuiciamiento Civil. Ley 1/2000, de 7 de enero. (*B.O.E.* núm. 7 de 8 de enero; corrección de errores en *B.O.E* núm. 90, de 14 de abril, (Publicado, en *BOE.* núm. 180, de 28 de julio)).

9. Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico. (Publicado, en *B.O.E*., núm. 166, de 12 de julio de 2002).

10. Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. (Publicado, en *BOE*, núm. 312, de 29 de diciembre de 2007, 19 p.).

11. Ley 16/2009, de 13 de noviembre, de Servicios de Pago. (*BOE.,* núm. 275, de 14 de noviembre de 2009).

12. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos (*BOE*. 298, de 14 de diciembre de 1999, 12 p.).

13. Ley 19/1985, de 16 de julio, Cambiaria y del Cheque (*BOE*, núm. 172, de 19 de julio de 1985, 14 p).

14. Real Decreto de 24 de julio de 1889, por el que se publica el Código civil, *BOE,* núm. 206 de 25 de julio de 1889.

15. Ley 21/2011, de 26 de julio, de dinero electrónico, que transpone al ordenamiento jurídico español la Directiva 2009/110/CE, de 16 de septiembre de 20 09, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión de dichas entidades, en *BOE*, núm. 179, 27 de julio de 2011, 20 p.

16. Ley 11/2007, de 22 de j unio, de "acceso electrónico de los ciudadanos a los Servicios Públicos, en *BOE* núm. 150, 23 junio 2007.

Universidad
Carlos III de Madrid

NORMATIVA COMUNITARIA

NORMATIVA COMUNITARIA

❖ *Recomendaciones*

1. Recomendación 87/598/CEE, de 8 de diciembre de 1987, «relativa a un código europeo de conducta referente a los pagos electrónicos», (*Diario Oficial* núm. L 365 de 24/12/1987, 0072-0076).

2. Recomendación 88/590/CEE, de 17 de noviembre de 1988. "relativa a los Sistemas de Pago y en particular a las relaciones entre titular y emisor de tarjetas. Publicada en el *DO* núm. L 317, de 24 de noviembre de 1988.

3. Recomendación 97/489/CE, publicada en *Diario Oficial* nº L 208/50, de 02/08/1997, pp. 0052-0058.

❖ *Directiva*

1. Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. (*DOCE* núm. L 095 de 2 de abril de 1993 p. 29-34).

2. Directiva 97/5/ CE, del Parlamento Europeo y del Consejo, de 27 de enero de 1997, relativa a la transferencias transfronterizas (*DOCE* L 275, de 14 de febrero de 19997).

3. Directiva 97/7/ CE, del Parlamento Europeo y del Consejo, de 20 de mayo de 19 97, relativa a l a protección de l os consumidores en materia de contratos a distancia (*DOCE*, núm. 144, de 4 de junio de 19997).

4. Directiva 1999/93/CE, de 19 de enero de 2000, el objetivo de esta directiva es mejorar los servicios de transferencia transfronterizas, ayudando al Instituto Monetario Europeo en su tarea de promover la eficacia de las transferencias transfronterizas. Publicada en el *DOCE* núm. L 13. 2000.

5. Directiva 2000/46/CE, del Parlamento Europeo y del Consejo de 18 de septiembre de 2000 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades. Publicado en *DOCE* nº. L 275, de 27 de octubre de 2000

6. Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007 “sobre servicios de pago en el mercado interior”, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE. (*DO*, L 319/ 1, de 5 de diciembre de 2007).

7. Directiva 2011/83/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo. Publicano, (*DOUE,* L 304/64, 22 de noviembre 2011).

8. Directiva 2009/110/CE, del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE, definí el dinero electrónico. Publicado en *DOUE,* L 267, 10 octubre de 2009.

Normativa extranjera comunitaria

❖ *Portugal*

1. Decreto-Ley nº 290-D/1999, de 2 de agosto, sobre régimen jurídico de los documentos electrónicos y de la firma electrónica, modificado por el Decreto-Ley nº 62/2003, de 3 de abril. Publicado en *Diario de la República*, n. º 79 (S. I - A), de 3 de Abril de 2003.
2. Decreto-Lei n. º 88/2009, sobre Documentos Electrónicos y Actos Jurídicos, de 9 de Abril, en *Diário da República*, 1. ª série — N. º 70 — 9 de Abril de 2009.

Universidad
Carlos III de Madrid

NORMATIVAS INTERNACIONAL EXTRANJERA NO COMUNITARIA

NORMATIVAS INTERNACIONALY EXTRANJERA NO COMUNITARIA

- *Argentina*

1. LEY 25.065, de tarjeta de crédito. Sancionada, 7 de diciembre de 1998. Promulgada parcialmente: enero 9 de 1999. B.O.: 14/01/99.

2. Ley 25.506 de firma digital, de 14 de noviembre de 2001. Publicada el 11 de Diciembre de 2001. [En Línea] Disponible en Internet: http:// www.sice.oas.org/e-comm/.../arg/arg25506.asp(última consultada, 20 de febrero de 2009).

- *Costa rica*

  Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 8454 de 30 de agosto de 2005. [En línea] disponible en Internet: http://www.archivonacional.go.cr/pdf/ley_8454.doc.(última consulta 23 de octubre de 2010).

- *Estado de Utah(Estados Unidos de América)*

  Ley del Estado de Utah sobre Firma Digital (Utah Digital Signature Act), de 27 de febrero de 1995 modificada en 1996, publicada en octubre de 1995 por *The American Bar Association's Information Security Committee* (*Comité de la ABA Science and Technology*

Section). [En Línea] disponible en Internet: http//: www.State.tu.us/ccjj (última consulta el 20 de febrero de 2012).

❖ *Guinea-Bissau*

1. «Código del Proceso Civil y Legislación Complementaria», en *Boletín Oficial,* núm. 41, de 13 de Octubre de 1993. [En línea] disponible en Internet:http://www.fdbissau.org/html_files/legislacao.html(última consulta 14 de mayo de 2012), 323 p.

2. «La Constitución de la Republica de Guinea-Bissau, probado el 16 de mayo de 198 4(y modificada en 1 996, por la Ley Constitucional nº 1/96», en *Boletín Oficial* núm. 50, de 16 de Diciembre de 1996).

3. «Código Penal (Decreto-Ley 4/93», en *Boletín Oficial* núm. 41, de 13 de Octubre de 1993(modificada por la Ley 2/2002, publicada en el *Boletín Oficial*, núm. 21 de 27 de mayo de 2002 y por el art. 13 de la ley 7/97, de 2 de diciembre, en *suplemento del Boletín Oficial* núm. 48 de diciembre de 1997).

4. Ley 1/97, de 19 de marzo de 1997, en *Suplemento del Boletín oficial,* núm. 12, de 24 de marzo de 1997, Bissau.

5. Resolución nº 1/94 del Consejo de E stado, que permite la adhesión de Guinea-Bissau a la OHADA. Publicado en *Boletín Oficial,* núm. 3. Suplemento, de 17 de Janeiro de 1994.

CEDEAO

Tratado de la CEDEAO. [En línea] disponible en Internet: http://www.comm.ecowas.int/sec/fr/docs/traite_revise.pdf(última consulta, 20 de mayo de 2012).

UEMOA

1. Tratado de la Unión Económica y Monetaria del África Occidental (UEMAO) [En línea] disponible en Internet: http://www.wipo.int/wipolex/es/other_treaties/details.jsp?group_id=24&treaty_id=313(última consulta, 14 de mayo de 2012).

2. Reglamento Nº15/2002/CM/UEMOA, *de sistema de pago de 19 de septiembre 2002*[En línea] disponible en Internet:

   http://www.bceao.int/IMG/pdf/Reglement_n_15_2002_CM_UEMOA_relatifaux_systemesde_paiement_dans_les_Etats_membres_de_l_UEMOA.pdf(última consulta, 24 de mayo de 2012).

3. Directiva 08/2002/CM/UEMOA, sobre *las medidas para promover la banca y el uso de medios de pago sin dinero en efectivo*.
   [En línea] disponible en
   Internet:http://www.bceao.int/Directive_n08_2002_CM_UEMOA.html
   (última consulta, 24 de mayo de 2012).

4. Instrucción nº 01 / 2006 / SP, de 31 Julio *2006 relativa a la emisión del dinero electrónico y las entidades de dinero electrónico*.
   [En línea] disponible en Internet:
   http://www.bceao.int/IMG/pdf/INSTRUCTION_N_o_01-2006-_SP_DU_31_JUILLET_2006.pdf (última consulta, 25 de noviembre de 2012).

OHADA

Ley Uniforme sobre Derecho General comercial. Ley uniforme sobre derecho general comercial de la OHADA [En línea] disponible en Internet:http://www.fdbissau.org/PDF_files/OHADA-COMERCIALGERAL-VERSAO_FINAL.pdf (última consulta, 25 de noviembre de 2012).

Universidad
Carlos III de Madrid

RECURSOS ELECTRÓNICOS

RECURSOS ELECTRÓNICOS

http://www.es.wikipedia.org/wiki/Sistema_de_pago_electrónico - 22k

http://www.digicash.nl Digicash and echas are trademarks, by Digicash

http://www.ecash.net

http://www.cybercash.com

http://www.mondex.com

http://www.verisign.com

http://www.verisign.es/ssl/index.html?sl=t55180249290000018m

http://www.virtual.unal.edu.co

http://www.secto.org

http://www.microsoft.com

http://www.ibm.com

http://www.netscape.com

http://www.westlaw.es

http://www.mastercard.com

http://www.fecemd.org

http://www.adigital.org

http://www.safescrypt.com/images/ssl1.gif

http://www.europa.eu

http://pages.ebay.es/Seguridad-en-eBay/pagar-con-confianza.html

http://www.seguridadenlared.org/52.html

http www.uemoa.int

http://www.indexmundi.com/map/?t=0&v=140&r=af&l=es

http://www.economywatch.com/economic-statistics/Guinea-Bissau/Internet Users/

http://www.ohada.com/textes.php?categorie=38

http://www.jurisint.org/ohada/text/text.01.sp.html

http://www.reingex.com/CEDEAO-Comunidad-Economica-Estados-Africa-Occidental.asp

http://www.exitoexportador.com/stats1.htm

http://www.wipo.int/wipolex/es/other_treaties/details.jsp?group_id=24&treatyid=313

http://www.crin.org/espanol/RM/ecowas.asp

http://www.stat-guinebissau.com/pais/index_quadro_fisico.htm

http://www.ikuska.com/Africa/economia/paises.htm

https://www.cia.gov/library/publications/the-world-factbook/geos/pu.html

http://www.ecowas.int/

https://observatorio.iti.upv.es/media/managedfiles/2008/11/06/ESTUDIO.pdf

http://www.itu.int/es/about/Pages/default.aspx

https://www.moneybookers.com/app/products.pl

http://corporate.skrill.com/

Universidad
Carlos III de Madrid

GLOSARIO

GLOSARIO

Antivirus. Programas que buscan detectar virus informáticos y otro tipo de software dañino, para eliminarlos o dejarlo sin efecto.

Algoritmo criptográfico. Una función matemática utilizada en combinación con una clave que se aplica a la información para asegurar la confidencialidad, la integridad de los datos y/o la autenticación. También se conoce como cifrar.

Autoridad de Certificación o Prestador de Servicio de Certificación *(Certification Authority en Inglés).* Es una entidad pública o privada que emite certificados digitales. Puede ser una entidad extranjera (como VeriSign que ofrecen servicios de certificación), o nacional.

Carga de la prueba: es el deber que tienen las partes de probar los hechos que alegan y afirman como fundamento y premisa de sus pretensiones, constituyendo una excepción este principio el sistema de presunción legal que operan en la legislación española.

Certificado digital (*en Inglés se conocen como public-key certifícate, digital certifícate o digital ID)*. Es el documento electrónico que vincula una clave pública y uno o más atributos relacionados con la identidad de la persona que posee la clave privada correspondiente. Los certificados digitales, además de ser documentos electrónicos, son documentos firmados digitalmente por un tercero. Como ejemplos de atributos vinculables en un

certificado digital, se puede citar: nombre, dirección de correo electrónico, datos bancarios, número de identidad fiscal, entre otras.

Cifrado. Es el proceso de transformar un texto o mensaje inteligible (en claro), en uno ininteligible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el algoritmo de cifrado para cada uso distinto

Comercio electrónico "*e-commerce*": transacciones comerciales en la red que se establecen entre empresas (B2B), entre consumido y empresa (B2C), o entre particulares (C2C).

Contrato. Es todo acuerdo de voluntades entre, al menos, dos sujetos de derecho por el que crean, modifican o extinguen relaciones jurídicas de crédito a deuda que se hallan al alcance de la autonomía de la voluntad. Para que exista contrato, las partes han de consentir sobre determinada causa y, en algunos casos excepcionales, materializando todo esto por escrito o por medios electrónicos.

Contrato de adhesión. Son aquellos contratos en que el contenido de los mismos está establecido por uno de los contratantes sin intervención o participación de la otra parte, que se limitará a dar su consentimiento a cuanto estableció la primera. Muchas veces, el contrato de adhesión ésta documentado en un formulario ya previsto.

Contrato electrónico. Todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

Contrato normativo. Son los que reglamentan otros posibles futuros contratos. En general, se celebran entre empresas o determinados grupos

de intereses que desean dejar convenidas las bases de futuros contratos. De esta manera, al celebrarse éstos, existen ya reglas de carácter privado que los disciplinan de manera uniforme. Los contratos normativos no obligan, pues, a celebrar nuevos contratos; sencillamente los prevén y, caso de celebrarse otros contratos por las personas obligadas por el contrato normativo, deberán atenerse a las reglas pactadas en éste. Un caso típico de contrato normativo es el denominado contrato de tarifa.

Contrato oneroso. Son los que impone una obligación a una o ambas partes contractuales.

Contrato sinalagmáticos. Son aquellos en los que cada parte contratante asume el papel o función de acreedor y deudor de la otra parte, como sucede en el contrato de compraventa. Por tanto, cada contratante asume, respecto de lo otro, alguna obligación bilateral o recíproca.

Criptografía. Es el arte o ciencia de cifrar y descifrar una determinada información de carácter confidencial mediante técnicas especiales. Es empleada frecuentemente para permitir un intercambio de mensajes que sólo pueden ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Criptoanálisis. Es el conjunto de procedimientos, procesos y métodos empleados para descifrar los textos cifrados sin conocer la clave.

Criptología. Es la ciencia que estudia los distintos sistemas de cifrados destinados a ocultar el significado del mensaje a otras personas que no sea el emisor y receptor de la misma.

Encriptar (*encrypt).* Transformar datos en un código secreto que puede ser descifrado únicamente por la parte interesada. Se utiliza para proteger archivos y correo electrónico de la vista de personas ajenas.

Intercambio electrónico de datos *(EDI).* El intercambio electrónico entre entidades comerciales (en algunos casos también administraciones públicas), en un formato estandarizado, de datos relacionados con una serie de categorías de m ensajes tales como pedidos, facturas, documentos aduaneros, avisos de remesas y pagos. Los mensajes EDI se envían por redes públicas de transmisión de datos o por canales del sistema bancario. Cualquier movimiento de fondos iniciado por medio de un EDI se refleja en instrucciones de pago que fluyen por el sistema bancario.

Cortafuego (*Firewall en Inglés*). Combinación de hardware y software para permitir sólo el acceso autorizado a funcionalidad del otro lado de la pared, y mantener la seguridad de una red. Puede ser implementado en un router o ser una combinación con hosts. También se usan dentro de las redes.

Firma electrónica. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Firma digital. Es una aplicación basada en la criptografía de clave pública, especialmente en el ámbito de l a contratación electrónica, en la que se proporciona autenticidad, integridad y no rechazo de l a información transmitida y de la identidad del transmitente en intercambios económicos en los que las partes no se conocen previamente.

Fraude. Engaño que se realiza eludiendo obligaciones legales o usurpando derechos con el fin de obtener un beneficio.

Función hash o resumen de texto. Es una función matemática que se aplica sobre un conjunto de datos o documentos de cualquier tamaño y, como resultado, se obtiene otro de t amaño reducido, en ocasiones denominado “resumen o digest” de los datos originales, de longitud fija (entre 128 ó 160 bits) e independiente de la longitud original.

Los Gateway (Pasarela de pago o Terminal de Punto de Venta Virtual). Mecanismo que procesa y autoriza las transacciones del proveedor de bienes o servicios en Internet, permite el cobro de las ventas realizadas en la red cuando el pago de las mismas es efectuado con tarjeta (crédito o débito). Los Gateway de pag o cifran información sensible, tal como números de tarjetas de crédito, para garantizar que la información pase en forma segura entre el cliente y el vendedor.

Hackers. Se usa para referirse a un experto en algunas ramas técnica relacionada con la informática: programación, redes de c omputadoras, sistemas operativos, hardware de r ed, entre otros. En general es más benigno que cracker, pero son variaciones del mismo tema.

Keylogger. Modalidad de troyano, cuyo mecanismo consiste en capturar las pulsaciones del teclado con el fin de obtener contraseñas u otra información confidencial del usuario.

Internet: una infraestructura de comunicación abierta y global que consiste en redes de computación interconectadas y que permite el acceso a información remota y el intercambio de i nformación entre computadoras / ordenadores.

Instrumentos de pago. Son aquellos mecanismos mediante los cuales se inicia la transferencia de di chos medios de pag o entre las partes intervinientes en una transacción.

Password: palabra o código que se usa para propósitos de seguridad contra accesos no autorizados a datos u otros aparatos. Es normalmente operado por el sistema operativo del DBMS (Data Base Management System). Sólo es posible para el computador verificar la contraseña, no al usuario.

Número de identificación Persona (PIN). Es un código numérico que el poseedor de una tarjeta puede necesitar introducir para la verificación de su identidad. En las operaciones electrónicas se ve como el equivalente de una firma.

Phisher. Es la expresión empleada para designar a l os estafadores que cometen fraudes de *phishing*.

Protocolo: procedimientos para el intercambio de mensajes electrónicos entre dispositivos de comunicación.

Red abierta: red de telecomunicaciones en la cual el acceso no es tá restringido.

Scams. Es la combinación de *phisher* y las cartas nigerianas. Consiste en ofertar trabajos con alta remuneración por chat, foros de discusión, pidiéndoles sus datos personales, número de s eguridad social y datos bancarios para así poder contratarlos

Servidor. Computador que proporciona servicios a través de una red a otros computadores u ordenadores.

Soporte duradero. Todo instrumento que permita al consumidor o al comerciante almacenar información que se le transmita personalmente de forma que en el futuro pueda recuperarla fácilmente durante un período de tiempo acorde con los fines de dicha información y que permita la reproducción de la información almacenada sin cambios.

Spoofing. Diferentes técnicas o métodos que utilizan los ciber-delincuentes (hackers) para la suplantación de identidad generalmente con fines maliciosos, por ejemplo, la suplantación de una tercera persona: su sitio web, su correo electrónico o s u identidad el ectrónica(la IP o c lave personal).

Spyware. Tipo de troyano o código malicioso usado habitualmente para espiar información confidencial de ordenadores privados, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legitimo del ordenador hace.

Texto en claro datos que no están cifrados y que por lo tanto se encuentran en un formato legible.

Uso fraudulento o indebido de la tarjeta de crédito. Implica el uso no autorizado de la información de la tarjeta por parte de un tercero con el propósito de cargar compras en la cuenta del titular de la misma o extraer fondos de su cuenta. El fraude o el uso fraudulento de la tarjeta de crédito está considerado como una forma de robo de identidad.

Vishing. Tipo de fraude con características muy similares al *phishing,* pero en vez de enviar e-mail se realizan llamadas telefónicas por Internet solicitando los números de las tarjetas de créditos, claves secretas, entre otras.